EXPERT INSIGHT

Mastering Microsoft Intune

Deploy Windows 11, Windows 365 via Microsoft Intune, Copilot and advance management via Intune Suite



Second Edition

Christiaan Brinkhoff | Per Larsen

Forewords by:

Steve Dispensa, CVP, Microsoft Intune

Scott Manchester, VP, Windows 365 and AVD

‹packt›

Mastering Microsoft Intune

Second Edition

Deploy Windows 11, Windows 365 via Microsoft Intune, Copilot and advance management via Intune Suite

Christiaan Brinkhoff

Per Larsen

BIRMINGHAM—MUMBAI

Mastering Microsoft Intune

Second Edition

Copyright © 2026 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Senior Publishing Product Manager: Reshma Raman
Acquisition Editor – Peer Reviews: Gaurav Gavas
Project Editor: Amisha Vathare
Content Development Editor: Soham Amburle
Copy Editor: Safis Editing
Technical Editor: Anjitha Murali
Proofreader: Safis Editing
Indexer: Subhalakshmi Govindhan
Presentation Designer: Ganesh Bhadwalkar
Developer Relations Marketing Executive: Meghal Patel

First published: October 2021
Second edition: March 2024

Production reference: 1120126

Published by Packt Publishing Ltd.
Grosvenor House
11 St Paul's Square
Birmingham
B3 1RB, UK.

ISBN 978-1-83546-851-7

www.packtpub.com

Forewords

By **Steve Dispensa**, *Corporate Vice President, Microsoft Intune*

Microsoft Intune

Since Christiaan and Per's first edition of *Mastering Microsoft Endpoint Manager*, a lot has changed, in the world and in the product. To begin with, MEM has gained its rightful name, Intune, Intune, and thus the title of this second edition no longer matches the first edition. (And note the lower-case "t" in "Intune" – Microsoft lore has it that every time someone writes "InTune" a unicorn dies.) We've moved from pandemic recovery to a world of hybrid work, however much some organizations insist employees come to the office every day. Geopolitical conflicts have fueled a rise in nation-state attacks on IT infrastructure – a rise that is likely to be permanent. And, unless you've been living under a rock the last year (and even if you have), you will have felt the effects of AI's coming of age.

Intune has changed too, and more than just in name. It is now the largest endpoint management solution in the world, larger than all other products in this space combined. The move to the cloud is proceeding apace, with almost two-thirds of the managed Windows PC population now managed in the cloud. Intune has gotten much richer support for macOS, and as of last year, it now supports Linux. It is also broadening its reach from its traditional focus on information workers, with new capabilities for frontline workers and their devices. ConfigMgr is still going strong, of course, but with these improvements in Intune's cloud-native reach, more customers than ever are choosing to move their endpoint management to the cloud.

As Intune has grown, customers have asked for help in solving problems that are adjacent to our core endpoint management mission. In response, we have released the Intune Suite, a set of six solutions that allow customers to unify and simplify their infrastructure, driving down complexity, reducing cost, and improving security. These new offerings are scenarios where Intune has a unique value proposition to offer. For example, Microsoft Cloud PKI is directly integrated into Intune and Entra and allows the direct replacement of legacy CA infrastructures with Microsoft's cloud-based scale, availability, and security.

The rise of AI may be the most profound change of all, not only since the last edition of this book, but since the dawn of the Internet itself. Generative AI has already revolutionized the way knowledge workers get their jobs done, the way students learn, and the way coders write software.

Soon, we will bring the power of generative AI to Copilot for Security and Copilot for Admins, which will be force multipliers for security and IT pros to help them scale their impact. Intune will be fully Copilot-enabled, making life easier for hundreds of thousands of end-user computing professionals around the globe.

Yes, the world has changed dramatically since 2021, and now, it's changing again as we create an AI-powered future. Every company, school, and individual in the world stands to benefit. These advances will be driven via the cloud, which hosts the enormous amounts of compute power and storage needed to deliver these new capabilities. And that brings us back to Intune. There has never been a better time or a more important reason to go cloud-native in your organization, and Christiaan and Per have written exactly the book to help you on your journey.

By **Scott Manchester**, *Vice President, Windows 365 + AVD*

The innovation engine that drives Windows in the cloud experience

Innovation can take many forms; as technology providers and product people, it's often difficult to put what we're building in context. And for many of us, we have a clear preference for the kinds of product areas we work on. When we develop products to meet the diverse needs of our customers, we are thoughtful in how we innovate. Consider there are three core types of innovation: **Disruptive**, **Evolutionary**, and **Revolutionary**. Let's walk through some examples of these types of innovation.



Consider the case of innovation on televisions; while the act of watching screen-based entertainment remained the same, LCD televisions built on existing technological frameworks and material advancements to deliver a new device type that made the act of consuming new content better than on traditional CRT-based TVs. This is a great example of an evolutionary advancement in televisions.

The Internet would be an example of a revolutionary advancement. It's changed how we buy, learn, and fundamentally communicate with each other. It has created new markets and significantly expanded others. The modern electrical vehicle is a disruptive technology. Consider 15 years ago the three leading US-based automakers were Chrysler, Ford, and Chevy. As of the time of writing, Tesla's market capitalization is around four times the size of all of these manufacturers combined. Tesla disrupted the market by offering new value, direct-to-consumer sales, and the ability to attach services to the sale after the initial purchase.

Let's discuss the forces that are shaping the innovation happening in the cloud virtualization world. The shift to hybrid work created new opportunities, but it also created new challenges. Things look different when the IT team isn't down the hall from employees who need help. New employees need to be onboarded, distributed teams need to be connected, specialized workloads need to be enabled, and new projects need to be scaled up. IT needs to on-ramp employees, but they also need to be prepared to respond to rapidly changing environments, while still maintaining business continuity. And, while managing this, IT also needs to ensure they are keeping their estate secure and meeting ever-changing regulatory requirements.

It is a challenge to address these needs with agility without overburdening IT, letting costs get out of control, sacrificing productivity, or compromising security. The changing nature of work is creating a tremendous opportunity for all of us in the virtualization market. Today Microsoft can deliver Windows to users in 3 ways: on a physical device, through Azure Virtual Desktop, and through Windows 365. When you think about the innovation framework we discussed earlier, we can talk about our approach to delivering a Windows cloud experience that innovates in response to the changing nature of work.

Azure Virtual Desktop is a cloud VDI product that was a natural evolution from traditional on-prem VDI. Cloud VDI provides a PaaS-based management plane and the ultimate flexibility in computing, storage, density, and location. We think about Azure Virtual Desktop as our "any" offering – any compute and storage combination, any location, and any supported OS. Admins that are familiar with deploying and managing traditional VDI will find Azure Virtual Desktop a huge step forward that brings the reach and capabilities of Azure to bear in addressing their virtualization needs.

Windows 365 is a truly revolutionary innovation: the cloud PC allows us to create a Software as a Service, or SaaS, offering that redefines the end-user experience and can be managed by an endpoint administrator using the same tools, baselines, and processes as a traditional PC. A cloud PC can be provisioned with Zero Touch, the security principles are based on Zero Trust, and end-users can immediately be productive with Zero Ramp. We affectionately refer to Windows 365 as the "zero" offering.

Thank you, Microsoft!

We also want to say a huge thank you to the following people at Microsoft who helped contribute to this book.

- **Steve Dispensa** and **Scott Manchester** for writing our forewords.
- **Phil Gerity** and **Justin Zarb**, our managers, for the support along the way!
- **Saurabh Bansal** and **Issa Khoury** from the Universal Print team
- **Lavanya Lakshman** from the AI – Copilot for Security team
- **Adam Nichols** from the Windows Autopatch/Windows Servicing and Delivery team
- **Matt Call** from the Microsoft Intune – Security team

We are also grateful to work at Microsoft, which supported us while writing this book. **#CommunityLove**

Contributors

About the authors

Christiaan Brinkhoff works as a Principal Program Manager and Community Director for Windows 365 and AVD at Microsoft. In his role at Microsoft, he works on features such as the Windows 365 app, Switch, and Boot, and lately he has also worked on Offline mode and the new Windows 10 ESU offering for Windows 365. Christiaan is also the author of 4 books and an inventor (with 4 patents). His mission is to drive innovation while bringing Windows 365, Windows, and Microsoft Intune closer together, and also drive community efforts around virtualization to empower Microsoft customers in leveraging new cloud virtualization scenarios. Christiaan joined Microsoft in 2018 as part of the FSLogix acquisition. He has also been awarded with the Microsoft MVP, Citrix CTP, and VMware Expert community achievements – for his continued support in the EUC community.

Per Larsen works as a Senior Product Manager in **Customer Experience Engineering** (**CxE**) – Microsoft Security Engineering. He plays a very crucial role in Microsoft in shaping and enhancing the product experience for customers. Per's focus is on driving strategy and roadmap conversations with Microsoft's most strategic customers. He also focuses heavily on driving insights and analyzing customer needs relating to security admin experience and Intune Suite product feedback.

Per is a frequent speaker at public events, conferences, and user groups on cloud-native Windows management.

He has also authored the book *Mastering Microsoft Endpoint Manager: Deploy and manage Windows 10, Windows 11, and Windows 365 on both physical and cloud PCs*.

Per joined Microsoft in 2019 working directly with the Intune engineering team. Prior to joining Microsoft, Per had more than 20 years of experience with device management. He has also been awarded Microsoft MVP thrice for all the exceptional community work he has done.

About the reviewers

Niall Brady is a blogger and an occasional speaker who focuses on step-by-step guides and videos for Windows 365, Intune, ConfigMgr, and more.

Niall is a 13-times Microsoft MVP (Enterprise Mobility, Windows, and Devices) based in Sweden but originally from Ireland. Niall has contributed toward several books on Configuration Manager and Intune and has even had his own book published (*The Windows-noob OSD Guides for Configuration Manager 2012 R2*).

Paul Winstanley is a 7-times Enterprise Mobility MVP who has 30 years of IT experience. He's spent the last 15 years specializing in endpoint management via Microsoft Configuration Manager and Microsoft Intune.

Paul is an independent consultant with his own endpoint management company, SCCM Solutions Ltd, which celebrated its tenth-anniversary last year, and works with customers all over the globe.

He blogs on his SCCMentor website, sharing his knowledge of Intune, Configuration Manager, Windows, MDM, and security, and is active on X, formerly known as Twitter, as @**sccmentor**.

Originally from Barnsley, in the North of England, he's lived in London for the past 30 years with his wife, four children, and brother-in-law.

Peter Daalmans is a Principal Workplace Architect and a Microsoft Certified Trainer at Daalmans Consulting B.V. with a primary focus on the modern management of Windows and mobile devices. He has been awarded Microsoft Security MVP (Configuration Manager/Microsoft Intune) every year since 2012.

He also writes blogs to share his knowledge on *MSIntune.blog*. Peter is also one of the founders and leads of the Workplace Ninja User Group, Netherlands. Along with that, he is also a part of the organizing team and the speaker manager of the Workplace Ninja Summit.

He has authored several books on Microsoft Configuration Manager and Microsoft Intune.

Peter speaks at local and international events, conferences like Microsoft Ignite, Microsoft TechEd (Australia/New Zealand), IT/Dev Connections, TechMentor, Techorama Belgium, **Midwest Management Summit** (**MMS**), BriForum (London, Denver, and Boston), TechDays Netherlands, and Experts Live Netherlands.

Learn more on Discord

To join the Discord community for this book – where you can share feedback, ask questions to the author, and learn about new releases – follow the QR code below:

`https://packt.link/SecNet`

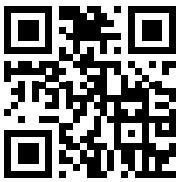


Table of Contents

Preface xxvii

Free Benefits with Your Book xxxii

Section I: Understanding the Basics 1

Chapter 1: Introduction to Microsoft 365 3

Microsoft 365 cloud services 4

What do these services achieve? • 4

Microsoft Intune • 4

Intune Suite • 7

AVD • 7

Windows 365 • 7

AVD and Windows 365 – what are the differences? • 8

Components that Microsoft manages and the customer manages • 9

Windows 11 • 10

Windows Copilot • 12

Security Copilot • 14

Intune Copilot • 14

Productivity Score • 15

Endpoint analytics • 16

Microsoft 365 Apps (for Enterprise) • 18

OneDrive for Business (part of Microsoft 365 Apps) • 18

Microsoft Teams • 19

Microsoft Edge • 20

Universal Print • 21

Microsoft Defender for Endpoint • 21

Exchange Online • 22

SharePoint Online • 22

Summary 23

Questions 23

Answers **23**
Further reading **24**

Chapter 2: Cloud-Native Endpoints 25

Paths to cloud native **25**
Microsoft Intune **26**
Intune admin center portal • 28
Microsoft 365 admin center portal • 28
Intune Partner portals • 29
Surface Management Portal • 29
HP Connect • 31
Windows 365 • 35
Microsoft Entra ID • 36
Cloud Management Gateway • 37
Compliance policies • 37
Windows Update policies • 37
Resource access policies • 38
Endpoint protection • 38
Device configuration • 39
Office Click-to-Run apps • 40
Client apps • 40
Microsoft Intune – from on-premises to the cloud • 42
Exploring Windows 11 Enterprise in detail **42**
Windows subscription activation • 43
Windows Autopatch • 44
Windows as a Service – update release cycle • 45
WUfB • 46
Who should use WUfB (now Autopatch)? • 47
Why do you want to leverage WUfB? • 47
What does WUfB allow me to configure? • 47
What is the WUfB deployment service? • 49
BYOD **49**
What is zero trust? **50**
Verifying identity • 50
Verifying devices • 50
Windows 365 for non-managed endpoints **52**
Summary **52**

Questions **52**
Answers **52**
Further reading **53**
Join the CloudPro Newsletter with 44000+ Subscribers **53**

Chapter 3: Requirements for Microsoft Intune *55*

Endpoint scenarios **56**
Identity roles and privileges for Microsoft Intune **56**
Using Intune filters when assigning **57**
Compliance Administrator • 59
Compliance Data Administrator • 59
Intune Administrator • 60
Message Center Reader • 60
Security Administrator • 60
Security Operator • 60
Security Reader • 60
Identity roles and privileges for a Windows 365 Cloud PC **61**
Azure Subscription Owner • 61
Domain Administrator • 61
Identity roles and privileges for Universal Print **61**
Licensing requirements **61**
Supported OSes **62**
Required web browser versions • 63
Windows 11 hardware requirements **63**
How do you get Windows 11? • 66
Intune Administrator Licensing **66**
Entra group-based licensing • 68
Setting the mobile device management authority • 68
Enabling Windows automatic enrollment • 69
Using Azure Virtual Desktop with Microsoft Intune • 71
Microsoft Intune device restrictions for Windows • 74
Blocking personal Windows devices • 76
Microsoft Intune device limit restrictions for Windows • 78
Customizing Intune Company Portal apps, the Company Portal website, and the Intune app • 80
Microsoft Intune – network URL firewall requirements **83**
Access for managed devices • 84
Network requirements for PowerShell scripts and Win32 apps • 86

Microsoft Store endpoint URLs • 88
Windows 365 endpoint URLs • 88
Windows Push Notification Services – required URLs • 88
Windows 365 and Azure Virtual Desktop – required URLs • 89
Universal Print – required URLs 89
Delivery Optimization • 90
Summary 90
Questions 90
Answers 91
Further reading 91

Section II: Windows 365 93

Chapter 4: What is Windows 365? 95

What is Windows 365? 96
Removing the complexity of traditional VDI deployments • 97
What to think about as a VDI administrator • 97
Removing complexity while increasing security • 97
Low costs as a fixed-price model • 97
The transition to modern management with Microsoft Intune • 98
Windows 10 ESUs • 99
Comparing Windows 365 Enterprise and Business • 100
What is Windows 365 Frontline? • 102
What is Windows 365 Government? • 103
Microsoft Intune • 103
High-level architecture components and responsibilities • 104
Configuration Manager support 105
Co-management and Windows 365 • 105
Disaster recovery • 107
Sizes and performance of fixed-price licenses • 108
GPU-Enhanced Cloud PCs 110
Connect to your on-premises network 111
Provisioning policies • 112
Windows 365 – gallery images • 113
Custom images • 114
Windows Updates via Autopatch • 114

Roles and delegation • 115
The Watchdog service • 117
Optimized Teams on Windows 365 • 119
Screen capture protection and watermarking • 119
Migrate GPOs to a Settings Catalog policy • 120
Summary **121**
Questions **122**
Answers **122**
Further reading **122**
Join the CloudPro Newsletter with 44000+ Subscribers **122**

Chapter 5: Deploying Windows 365 123

Technical requirements for deploying Windows 365 ..... **124**
Required URLs • 124
RDP requirements and optimizations • 127
Connect to on-premises networks (optional) • 128
Purchasing and assigning Cloud PC licenses • 132
Provision a Cloud PC **133**
Image management – creating a custom image (optional) • 140
Reprovisioning a Cloud PC • 148
Local administrator permissions • 149
Security baselines for a Cloud PC • 149
Zero Trust: Conditional Access management for Cloud PCs **150**
Connecting to your Cloud PC • 152
Windows App • 152
Deploy Windows App via Intune **156**
Windows App – User Actions • 159
Bulk User Actions via Intune **160**
Supported redirections per endpoint platform • 160
Windows 365 Boot shared mode **163**
Windows 365 Boot dedicated mode **174**
What if you have multiple Cloud PCs? **174**
Battery status redirection **175**
Windows 365 Switch **176**
Resize Cloud PCs • 178
Bulk device actions **179**
Monitoring and analytics **181**

Intune Suite – Endpoint Privilege Management • 182
Intune Suite – Enterprise App Management • 183
Intune Suite – Remote Help • 184
Want to dive deeper into Windows 365? **184**
Summary **185**
Questions **186**
Answers **186**
Further reading **186**

Section III: Mastering Microsoft Intune 187

Chapter 6: Windows Deployment and Management 189

Deploying existing Windows devices into Microsoft Intune **189**
Enrolling devices – Windows enrollment • 190
Automatic enrollment • 191
Testing company domain CNAME registration for Windows enrollment • 191
Enrollment Status Page • 193
Enrollment notifications • 194
Windows Autopilot • 200
What about existing infrastructure? • 201
Co-management and tenant attach • 201
Co-management settings • 208
Windows Update for Business **210**
Types of updates managed by Windows Update for Business • 210
Enforcing compliance deadlines for updates • 211
How to handle conflicting or legacy policies • 211
How to set up and configure Windows Update for Business • 212
Safeguard holds • 223
Feature updates for Windows 10 and later **224**
Opting out of safeguard holds • 229
Expediting a Windows patch • 231
The Windows Insider Program for Business • 235
Updating Microsoft 365 apps • 238
Windows Autopatch **238**
Windows Autopatch requirements • 239
How to enable Windows Autopatch • 239

Optimizing Windows Update rings • 242
Enabling Windows Autopatch for Cloud PCs • 244
Summary **244**
Questions **245**
Answers **245**
Further reading **245**
Join the CloudPro Newsletter with 44000+ Subscribers **246**

Chapter 7: Windows Autopilot 247

Technical requirements **247**
Windows Autopilot overview **248**
Uploading the hardware ID to Windows Autopilot **250**
Where is Windows Autopilot device information stored? • 257
Windows Autopilot for existing devices **259**
Windows updates during the OOBE **264**
Auto-assigning Windows Autopilot profiles in Intune • 265
Signing in to Graph Explorer • 266
Enrollment Status Page (ESP) **272**
ESP implementation – Windows CSP • 272
Autopilot reporting and diagnostics **275**
Company Portal • 279
Configuring automatic BitLocker encryption for Autopilot devices • 281
Troubleshooting automatic BitLocker encryption on a VM **290**
Windows Hello for Business **290**
Cloud configuration scenario **295**
Introduction • 296
What you will need to continue • 297
Basics • 297
Resources to be created • 298
Apps • 299
Assignments • 300
Deploying • 301
Deploying essentials that users might need to access work or school resources • 303
Monitoring your cloud configuration devices • 303
SharedPC self-deployment scenario **303**
Creating a specific ESP for the SharedPC device • 303
Creating a Windows Autopilot profile • 305

Self-Deploying (preview) • 306
Creating a custom Windows profile to disable user ESP • 307
Creating a custom Windows 10 profile to disable FirstLogonAnimation • 307
Creating a Windows template SharedPC profile • 308
SharedPC technical reference • 310
Troubleshooting SharedPC • 312
Windows Autopilot Reset • 312
Wiping and resetting your devices 314
Fresh Start 315
Windows Recovery Environment • 316
Summary 316
Questions 316
Answers 317
Further reading 317

Chapter 8: Application Management and Delivery 319

Application delivery via Microsoft Intune 319
Different application types you can deploy 320
LOB applications • 322
MSI – via the LOB app • 322
MSIX – via the LOB app • 322
AppX – via the LOB app • 322
IntuneWin – via the Windows app (Win32) • 328
Supersedence mode • 342
Deploying Microsoft 365 apps 347
Update channels • 348
Office Customization Tool • 350
Microsoft 365 Apps admin center • 352
Getting started • 355
Device selection criteria • 355
Update exclusion dates • 356
Update deadline • 357
Microsoft 365 app customization • 360
Deploying Microsoft Teams 361
Deploying OneDrive 364
Deploying Microsoft Edge • 365
What is WinGet? 368

What is MSIX? **372**
AppxManifest.xml • 374
AppxBlockMap.xml • 374
AppxSignature.p7x • 374
How to create MSIX packages • 374
Pushing the MSIX package application to your endpoints • 382
Summary **385**
Questions **386**
Answers **386**
Further reading **386**
Join the CloudPro Newsletter with 44000+ Subscribers **386**

Chapter 9: Understanding Policy Management 387

Policy management **387**
What is a CSP policy? **389**
Windows Push Notification Service (WNS) **393**
Getting started with policy design **398**
Migrating existing policies from AD – Group Policy management **401**
Summary **409**
Questions **409**
Answers **409**
Further reading **409**

Chapter 10: Advanced Policy Management 411

Policy management **412**
Configuring a policy from the Microsoft Intune Security blade • 412
Configuring your Endpoint Security profile • 415
Microsoft Defender policy • 416
Antivirus reporting in Endpoint security • 418
Unhealthy endpoints • 418
Attack surface reduction • 419
Configuring a policy from the Settings catalog • 422
How do they work? • 432
Importing ADMX **438**
Configuring administrative templates **444**
OneDrive Known Folder Move configuration • 446
OneDrive – block syncing specific file extensions **450**

Configure device configuration (template) **451**
Leveraging a custom policy as a last resort • 453
Config Refresh **455**
Pushing PowerShell scripts – scripted actions to endpoints **456**
Multi admin approval **459**
Compliance policies **463**
Windows compliance policy • 464
Organizational compliance report • 469
Device compliance trends • 472
Device diagnostics settings • 472
Summary **474**
Questions **474**
Answers **475**
Further reading **475**
Join the CloudPro Newsletter with 44000+ Subscribers **476**

Chapter 11: Intune Suite 477

What is Intune Suite? **477**
Prerequisites • 479
How to get started with Intune Suite **479**
Specialty Device Management **481**
Endpoint Privileged Management **481**
How to configure EPM • 481
How to onboard devices to EPM • 482
Reusable settings • 486
Creating an EPM elevation rules policy • 491
Monitoring EPM events • 499
Elevation report • 499
Managed elevation report • 500
Elevation report by applications • 500
Elevation report by Publisher • 501
Elevation report by User • 501
EPM Agent • 502
How do you get your users' account type to Standard? • 502
Configure policy for standard user • 503
End user process • 505
Enterprise App Management • 508

Installing applications via Enterprise App Management • 509
What about enhanced application updates? • 517
Cloud certificate management (Cloud PKI) 522
How does the process work? • 523
Two-tier PKI hierarchy • 524
Certificate Revocation • 535
Ensuring trust and authentication: • 535
Reasons for certificate revocation: • 535
Practical scenarios: • 536
Remote Help for Windows • 546
How to enable Remote Help • 546
Configuring Remote Help in Intune • 547
How does Remote Help look from an end user's perspective? • 550
How do you remotely access a managed device? • 552
Remote Help Windows Firewall setup • 554
Conditional Access for Remote Help • 557
How to use Remote Help as an end user and as a ServiceDesk user • 563
Advanced Endpoint Analytics • 563
Device query • 567
Battery health • 570
Why Windows 365 and Intune Suite are a great combination • 572
Summary 573
Questions 574
Answers 574
Further reading 574

Chapter 12: Copilot/AI 575

The future of AI in Windows and Intune 575
Copilot in Windows 576
What can you use Windows Copilot for? 577
Direct instructions • 579
Questions • 579
Security Copilot (Device Management) 582
Intune policy generation via Security Copilot 582
Copilot assistant for Intune device queries 588
Troubleshooting Intune via Security Copilot 588
Troubleshooting • 589

Summary **591**
Questions **591**
Answers **591**
Further reading **592**
Join the CloudPro Newsletter with 44000+ Subscribers **592**

Chapter 13: Identity and Security Management 593

Microsoft Identity **593**
Entra ID **595**
Entra ID join • 595
Hybrid Entra ID join • 596
Entra ID users • 601
Entra ID guest users • 602
Entra ID group types • 603
Entra ID group membership types • 603
Conditional Access **605**
What is it? • 606
What are the common signals? • 606
What are the common decisions? • 606
Users and groups • 607
Cloud apps **608**
Conditions • 610
Grant **612**
Preventing users from carrying out Entra ID device registration **616**
Self-service Password Reset **617**
Entra ID password protection **618**
Passwordless authentication **619**
Enabling passwordless authentication **622**
What is and isn't supported in each passwordless scenario • 624
Passkeys **626**
How do passkeys work? • 626
How does it relate to passwords? • 627
How to enable passkeys • 627
Manage your passkeys • 629
Web sign-in **630**
BitLocker disk encryption **632**
BitLocker recovery keys **633**

Personal Data Encryption **636**
Windows Local Administrator Password Solution • 638
Application Control for Business • 644
Microsoft Defender for Endpoint **659**
Integration with Microsoft Intune • 659
Security baselines **660**
Compliance policies **661**
Windows 365 security baselines **663**
Microsoft Defender for Endpoint • 663
Connecting to Intune – Microsoft Intune integration **667**
Alerts and security assessments **676**
Security recommendations • 676
Defender keylogger protection **676**
Windows 365: customer-managed keys support for data encryption • 677
Screen capture protection and watermarking • 678
Summary **679**
Questions **679**
Answers **680**
Further reading **680**

Chapter 14: Monitoring and Endpoint Analytics 681

Endpoint analytics **682**
Cloud PC overview **683**
Cloud attached devices (preview) **684**
Endpoint analytics – Advanced Monitoring **684**
Startup performance – logon duration • 686
Performance score breakdown • 687
Resize cloud PCs • 690
Top 10 processes impacting Startup performance **692**
OS restart history **694**
Resource performance **694**
Insights and recommendations – score trends **695**
Application reliability **695**
Windows 365-specific metrics **696**
Insights and recommendations **698**
Configuration Manager data collection • 699
Customizing your baselines **700**

Remediations • 701
Windows 365 Frontline • 704
Azure Monitor integration • 705
System alerts and email notifications 706
Configure notifications for failed provisioning of cloud PCs • 706
Service health 709
Advanced Endpoint analytics 710
ControlUp Enrich 712
Summary 712
Questions 713
Answers 713
Further reading 713
Join the CloudPro Newsletter with 44000+ Subscribers 713

Chapter 15: Universal Print 715

What is Universal Print? 715
Universal Print – architecture overview • 717
Print clients – Universal Print for Windows • 718
Print clients – Universal Print for Mac • 718
Print clients – Web applications and print APIs • 719
Printers – Universal Print ready printers • 719
Printers – Universal Print connector • 722
Printer shares • 723
Printer defaults • 724
Is Universal Print secure and where does my printed data go? 724
Data Residency • 725
Data security • 726
Compliance and certifications • 726
Printer share access check • 727
Secure release • 727
Universal Print – requirements 728
End user requirements • 728
Admin requirements for managing Universal Print • 729
Managing print requirements • 729
Universal Print – requirements • 729
Network requirements • 730
Commercial cloud • 730

US government GCC cloud • 730
US government GCC-High cloud • 731
Network isolation and zero-trust • 731
Learning how to deploy Universal Print 731
Printer management – custom roles • 732
Connecting your existing printer to Universal Print • 733
Configuring Universal Print • 734
Log in to the Universal Print admin portal • 734
Register a Universal Print ready printer • 735
Register printer(s) with the Universal Print connector • 739
Enable hybrid Entra ID configuration via the Universal Print connector • 744
Create a printer share for the printer • 745
Test your Universal Print printer and printer share • 749
Assigning and deploying cloud printers with Microsoft Intune • 752
Summary 755
Questions 755
Answers 756
Further reading 756

Section IV: Troubleshooting and Community 757

Chapter 16: Troubleshooting Microsoft Intune 759

Chapter 17: Troubleshooting Windows 365 761

Chapter 18: Community Help 763

Community hall of fame 763
CAUTION! • 763
Community events to participate in! 767
MMS – Minnesota and Fort Lauderdale 768
MEM Summit – Paris 768
Workplace Ninja Summit – Europe 769
Windows 365 Community 769
Windows in the Cloud – video webcast 769
Summary 770

Chapter 19: Unlock Your Exclusive Benefits **771**

Other Books You May Enjoy **777**

Index **781**

Preface

The slow adoption of modern work solutions, which are designed to streamline the management of your environment, can often be attributed to a lack of understanding and familiarity with the product. This book will provide you with all the information you need to successfully transition to Microsoft Intune

Mastering Microsoft Intune explains various concepts in detail to give you the clarity to plan how to use **Microsoft Intune** and eliminate potential migration challenges beforehand. You'll get to master Cloud Computing services such as Windows 365 Cloud PC, the Intune Suite, Windows Autopatch, Windows Autopilot, Profile Management, Monitoring and Analytics, Universal Print, and much more!

The book will take you through the latest features and new Microsoft cloud services to help you to get to grips with the fundamentals of Intune and understand which services you can manage. Whether you need familiarity with physical or cloud endpoints, it's all covered.

By the end of the book, you'll be able to set up Intune and use it to run Windows and Windows 365 efficiently via Intune with all the latest features included!

What you will learn:

- Simplify the deployment of Windows in the cloud with Windows 365 Cloud PC.
- Deliver next-generation security features with the Intune Suite.
- Simplify Windows updates with Windows Autopatch.
- Configure advanced policy management within Intune.
- Discover modern profile management and migration options for physical and cloud PCs.
- Harden security with baseline settings and other security best practices.
- Find troubleshooting tips and tricks for Intune, Windows 365 Cloud PC, and more.
- Discover deployment best practices for physical and cloud-managed endpoints.
- Keep up with the Microsoft community and discover a list of MVPs to follow.

Who this book is for

If you are an IT professional, enterprise mobility administrator, architect, or consultant looking to learn about managing Windows on both physical and cloud endpoints for remote working via Intune, this book is for you.

What this book covers

Chapter 1, Introduction to Microsoft 365, teaches you about keeping your resources secure while leveraging other services within Microsoft 365's broader product suite. Understanding the fundamentals of a product is the most important factor for a successful deployment.

Chapter 2, Cloud-Native Endpoints, acknowledges how the basics of modern management are sometimes complicated to understand, and so you will learn about the concept of modern management and zero trust with Intune, the history, and the architectural concept to get a clear understanding of how all the devices from physical, virtual, and mobile all come together in one management console.

Chapter 3, Requirements for Microsoft Intune, provides a clear understanding of the different requirements for Intune, from OS versions and URL firewall allow-listing to the required licenses and privileges.

Chapter 4, What Is Windows 365?, teaches you everything you need to know to get started with this Microsoft cloud service and its latest new features such as Windows 365 Boot and Switch, which simplify deployment as well as your cloud PC maintenance with Intune.

Chapter 5, Deploying Windows 365, teaches you everything you need to know about how to deploy Windows 365, what the requirements are, and tips and tricks.

Chapter 6, Windows Deployment and Management, teaches you about deploying Windows Enterprise with Intune.

Chapter 7, Windows Autopilot, teaches you how and when to use Autopilot to enroll Windows on your physical endpoint devices. What are the recommended approaches and decisions to make beforehand? You will get to know all of this in this chapter.

Chapter 8, Application Management and Delivery, teaches you best practices to deploy and manage your Microsoft 365 and line-of-business applications on your Windows 10 endpoints.

Chapter 9, Understanding Policy Management, teaches you about the different policy types, what modern policy management means, and how it works on Windows 10/11 clients compared to Group Policy.

*Chapter 10, Advanced Policy Management, i*n extension to the previous chapter, will take a deeper look at policy management for Windows 10/11 and share the nuts and bolts of managing Windows and other tips and tricks.

Chapter 11, Intune Suite, teaches you about the new Intune Suite products in depth and what all the modules such as **Endpoint Privilege Management** (**EPM**), Enterprise App Management, Advanced Analytics, and Remote Help mean for you from both a business and technical perspective.

Chapter 12, Copilot/AI, teaches you about Microsoft's latest new generative AI functionalities for both Windows and Microsoft Intune via the Windows and Security Copilot integrations.

Chapter 13, Identity and Security Management, teaches you how to configure Azure Active Directory in the most secure way possible for your end users and IT department. You will learn what the different options to enable Azure MFA are, about BitLocker, and how to configure Microsoft Defender for Endpoint with end-to-end security-level integration in Intune.

Chapter 14, Monitoring and Endpoint Analytics, looks at how, after deploying your desktops, it's important to ensure the performance, logon duration segmentation, and quality level of Windows and applications. You will learn, in this chapter, how you can achieve this with Endpoint Analytics, Productivity Score, and other monitoring capabilities of Intune.

Chapter 15, Universal Print, looks at Universal Print and how, despite businesses doing more and more things in a digital way, printing on physical paper remains important. Universal Print is a relatively new platform service on Azure that can simplify the whole printing configuration and maintenance process compared to a traditional print server environment.

Chapter 16, Troubleshooting Microsoft Intune (Bonus Chapter – Online Content), teaches the most common causes and fixes of deploying Windows 10 Enterprise and other tips and tricks to unblock deployments to go smoothly. Both writers have over 2 decades of field experience in deploying Windows in many forms that they will share in this section.

Chapter 17, Troubleshooting Windows 365 (Bonus Chapter – Online Content), teaches you about all the different troubleshooting errors of Windows 365 Cloud PC to prepare you to respond proactively to any errors that could occur while deploying cloud PCs in your environment.

Chapter 18, Community Help, shares, as the writers have a strong community background, some of the best community events with Microsoft MVPs, and some of the best community blogs out there; some are written by beginners, while some are by Microsoft MVPs

To get the most out of this book

In order to get the most out of this book, it would be good to have a base-level understanding of Intune, Azure, Microsoft 365 cloud services, and so on. This is not required, however, as you'll learn all you need to know in this book!

Download the color images

We also provide a PDF file that has color images of the screenshots and diagrams used in this book. You can download it here: `https://packt.link/gbp/9781835468517`.

Conventions used

There are a number of text conventions used throughout this book.

`Code in text`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. Here is an example: "Enter `Device type restriction - HR` as the name."

A block of code is set as follows:

```
<?xml version="1.0"?>
<HardwareReport>
    <HardwareInventory>
         <p n="ToolVersion" v="3" />
         <p n="HardwareInventoryVersion" v="131" />
```

Any command-line input or output is written as follows and are indicated as command-line commands in the main body of the text:

```
msiexec /i " RemoteDesktop_1.2.1755.0_x64.msi" /qn ALLUSERS=2
MSIINSTALLPERUSER=1
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For instance, words in menus or dialog boxes appear in **bold**. Here is an example: "Go to **Tenant admin** | **Roles** | **Administrator Licensing**."



Warnings or important notes appear like this.



Tips and tricks appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, email us at `customercare@packtpub.com` and mention the book title in the subject of your message.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packtpub.com/support/errata` and fill in the form.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Share your thoughts

Once you've read *Mastering Microsoft Intune, Second Edition*, we'd love to hear your thoughts! Please `click here to go straight to the Amazon review page` for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Free Benefits with Your Book

This book comes with free benefits to support your learning. Activate them now for instant access (see the "*How to Unlock*" section for instructions).

Here's a quick overview of what you can instantly unlock with your purchase:

PDF and ePub Copies



- Access a DRM-free PDF copy of this book to read anywhere, on any device.
- Use a DRM-free ePub version with your favorite e-reader.

Next-Gen Web-Based Reader



- **Multi-device progress sync**: Pick up where you left off, on any device.
- **Highlighting and notetaking**: Capture ideas and turn reading into lasting knowledge.
- **Bookmarking**: Save and revisit key sections whenever you need them.
- **Dark mode**: Reduce eye strain by switching to dark or sepia themes.

How to Unlock

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.



Note: Keep your invoice handy. Purchases made directly from Packt don't require one

Stay Sharp in Cloud and DevOps – Join 44,000+ Subscribers of CloudPro

CloudPro is a weekly newsletter for cloud professionals who want to stay current on the fast-evolving world of cloud computing, DevOps, and infrastructure engineering.

Every issue delivers focused, high-signal content on topics like:

- AWS, GCP & multi-cloud architecture
- Containers, Kubernetes & orchestration
- Infrastructure as Code (IaC) with Terraform, Pulumi, etc.
- Platform engineering & automation workflows
- Observability, performance tuning, and reliability best practices

Whether you're a cloud engineer, SRE, DevOps practitioner, or platform lead, CloudPro helps you stay on top of what matters, without the noise.

Scan the QR code to join for free and get weekly insights straight to your inbox:



https://packt.link/cloudpro

Section I

Understanding the Basics

In this section, you will learn the fundamentals of the different Microsoft 365 services, what the benefits are, and how they are different in comparison to other technologies and services on the market.

This part of the book comprises the following chapters:

- *Chapter 1, Introduction to Microsoft 365*
- *Chapter 2 Cloud-Native Endpoints*
- *Chapter 3, Requirements for Microsoft Intune*

1

Introduction to Microsoft 365

Understanding the fundamentals of a product is the most important thing for a successful deployment. Keeping your resources secure while leveraging other services within the Microsoft 365 product suite is what you will learn about in this chapter.

In this chapter, we'll go through the following topics:

- Microsoft 365 cloud services
- Microsoft Intune
- Intune Suite
- **Azure Virtual Desktop** (**AVD**) and Windows 365
- Windows 11
- Windows Copilot
- Security Copilot
- Endpoint analytics
- Productivity Score
- Universal Print
- Microsoft Defender for Endpoint
- Microsoft Teams
- Edge
- Exchange Online
- SharePoint Online

Free Benefits with Your Book

Your purchase includes a free PDF copy of this book along with other exclusive benefits. Check the *Free Benefits with Your Book* section in the Preface to unlock them instantly and maximize your learning experience.

Microsoft 365 cloud services

Microsoft 365 cloud services (hereafter referred to as Microsoft 365) includes many services that you might use in your day job, whether as an IT professional or a non-technical user. These services help you to become more productive by simplifying tasks that would require a lot of work in on-premises environments.

A great example would be the shift we've made from Exchange Server to Exchange Online and of course now the shift of Windows to Windows 365, which is Microsoft's latest cloud service that allows enterprises and small businesses to leverage the power of Azure computing in Windows to improve the performance, scalability, and productivity of users across any device, any platform!

What do these services achieve?

In this introductory section of the book, we will briefly explain the core Microsoft 365 services and features that are relevant to the subject of this book, just to get a good baseline understanding of the differences between the various services. You'll also learn about the purpose and benefits of each service.

Microsoft Intune

Microsoft Intune is a family of products and services that helps businesses manage and maintain all their devices, regardless of whether it's a physical device, or a cloud-connected device endpoint.

The Intune family includes:

- Microsoft Intune
- Configuration Manager and co-management
- Endpoint analytics
- Windows Autopilot
- Intune admin center
- Intune Suite

Microsoft Intune provides a holistic management experience while adding new functionality and intelligent actions, such as anomaly detection in Advanced Endpoint Analytics and remediation scripts that can proactively resolve end user issues before they see an issue – without any complex migration or disruption of productivity.

It provides several assets to aid your transition to modern management while also increasing customers' security and helping them move to the cloud. Microsoft Intune also includes management capabilities for different endpoints. To summarize:

1. Windows
2. Android
3. Linux
4. macOS
5. iPadOS

The figure below explains all the management features Microsoft Intune delivers:

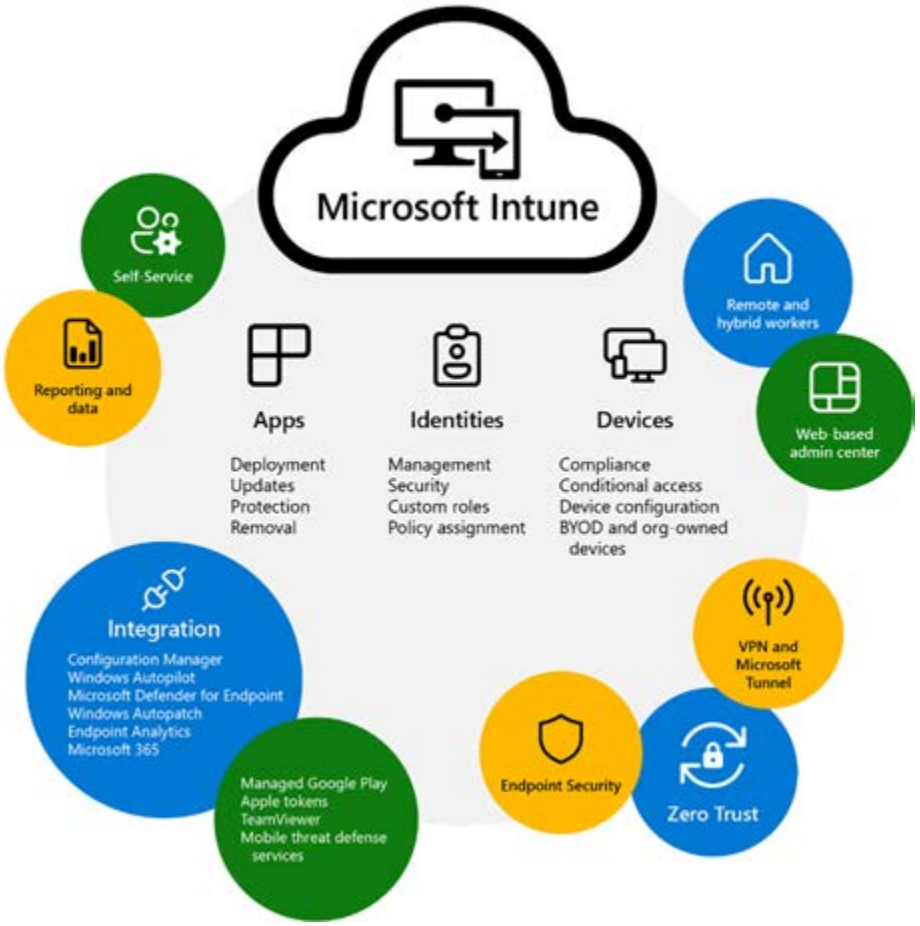


Figure 1.1: Microsoft Intune – service portfolio

Microsoft Intune helps you manage physical and Cloud PC endpoints, laptops, tablets, and other mobile devices, including iOS, Android, and macOS devices.

Microsoft Intune is built on **Entra ID** (**formally known as Azure Active Directory**) as the identity store for users and user/device groups; this also means that Intune relies 100% on Entra ID. It replaces the traditional Active Directory, includes hybrid identity capabilities, and can also integrate with local management infrastructures such as Configuration Manager via Kerberos.

Intune is applicable for devices that don't fall in the management scope of Group Policy, such as mobile phones, devices that are not **Active Directory Domain Services** (**AD DS**) domain members, or Windows 11 devices that are joined to Entra ID:

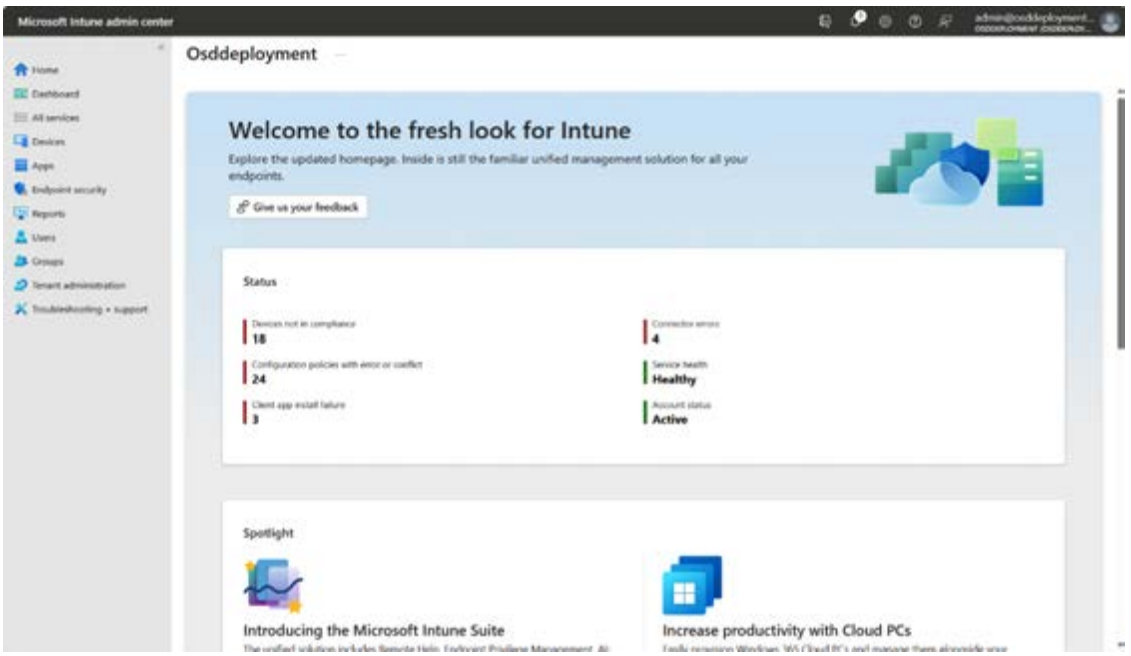


Figure 1.2: Microsoft Intune – admin center

With Microsoft Intune, you can achieve the following:

- Let your organization's employees use their physical and Cloud PC endpoint devices to access organizational data (commonly known as **Bring Your Own Device** (**BYOD**)).
- Manage organization-owned phones.
- Control access to Microsoft 365 from unmanaged devices, such as public kiosks and mobile devices.
- Help ensure that devices and apps that do connect to corporate data comply with security policies.

For example, when a user attempts to open one of their **Line-of-Business** (**LOB**) apps on their phone or Windows endpoint, Microsoft 365 checks with Entra ID to authenticate the user and verify whether that user can access the data from that app on that device. The granting of access depends on the following:

- Conditional Access policies defined within Entra ID
- Whether the app on that device complies with app configuration and data protection policies (Intune will confirm this for Entra ID)

If the device and app are both compliant with all applicable policies, Entra ID tells Microsoft 365 that the data can be accessed.

This concludes the Intune section; next, we will go into the new Microsoft Intune Suite.

Intune Suite

The Microsoft Intune Suite is a comprehensive new add-on platform to the Intune core service that consolidates critical advanced endpoint management and security solutions. Its design aims to streamline the customer's experience in managing endpoints, enhance their security stance, and deliver superior user experiences.

The Microsoft Intune Suite offers several key features:

- It deeply integrates with Microsoft Security and Microsoft 365.
- It equips IT and security teams with data science and AI tools to boost automation.
- It addresses challenges related to endpoint management, such as application packaging, and certificate management, and security issues such as end users being local administrators.

The suite's functionalities are integrated with Microsoft 365 and Microsoft Security across endpoint platforms, catering to both cloud and on-premises co-managed devices. The Intune Suite encompasses Remote Help (standalone) and all features included in Intune Plan 2.

AVD

AVD is a Microsoft-managed platform-as-a-service offering on top of the Microsoft Azure cloud. Unlike traditional **Virtual Desktop Infrastructure** (**VDI**) deployments, all hardware and all the infrastructure services, such as brokering, web access, load balancing, management, and monitoring, are all set up for you as part of a control plane offering. However, you would still need to configure them yourself on Azure, which means that there is a need for both Azure and VDI expertise in your business. This is where Windows 365 is different, as every Modern Desktop IT admin would be able to manage and maintain Cloud PCs – without the need for VDI and Azure expertise.

This concludes the section on AVD. In the next section, we will cover Windows 365.

Windows 365

Windows 365 is the world's first Cloud PC service that's designed for your hybrid work needs. Windows 365 is a new cloud service from Microsoft that securely streams your personalized Windows desktop, apps, and content from the Microsoft cloud (Microsoft Azure) to any device, anywhere. Windows 365 uses all the familiar security features implemented for physical Windows PCs to Cloud PCs to ensure safe and secure streaming. It is a revolutionary technology where both the IT admin and end user experiences are fundamentally different from traditional VDI and Cloud VDI. It combines the best of Windows, Azure, and Microsoft 365 to deliver simplified IT and modern end user experiences – providing an easy onramp for both existing and new customers.

A Cloud PC is the end user's own personal computer in the cloud that's optimized, scalable, and has high availability, all with a familiar Windows desktop experience. It's hosted in the Windows 365 service and is accessible from anywhere, on any device. A Cloud PC signifies the transformation of Windows from a device-centric **Operating System** (**OS**) to a hybrid personalized computing platform.

This means that you can burst your resources to the cloud via our Azure compute backend data centers without the need to configure it yourself! This shift of Windows into a blend of local and cloud OS opens up new opportunities for organizations of all scales via the CPU, GPU, and NPU for **Artificial Intelligence** (**AI**)-based workloads. With Windows 365, Windows becomes a dual local and cloud OS. Organizations have the liberty to decide whether a traditional PC with a locally installed OS or a Cloud PC with a cloud-based OS is more suitable for a specific user or role. In certain scenarios, a user might find it advantageous to have both a local and cloud OS, selecting the appropriate one for the task at hand.

Windows 365 is suitable for organizations of all sizes that need highly secure and agile hybrid work solutions. These are valuable for elastic workforces, distributed employees, and specialized workloads that require versatile compute and storage capabilities, accessible on any device. IT administrators can swiftly scale and resize Cloud PCs to meet the changing needs of their users and have the compute power and storage they need, with predictable costs. As an example, if a user in finance gets a new application that needs more compute power (CPU), then the IT admin can resize the Cloud PC for the user. Hybrid work use cases that can be supported effectively with Windows 365 include:

- Data access and security across devices, locations
- High-capacity computing
- **Bring Your Own PC** (**BYOPC**) environments
- Disaster preparedness and recovery
- Temporary workforces
- Mergers and acquisitions

AVD and Windows 365 – what are the differences?

Windows 365 is engineered for ease of use, enabling customers to enjoy the advantages of personalized Cloud PCs without the need for VDI or Azure expertise. It offers a predictable pricing model based on per-user and per-month charges, simplifying cost management. Windows 365 is ideal for customers who are not heavily invested in VDI or have virtualization expertise/resources, or for those who want to simplify their VDI infrastructure and prefer a fixed-cost, as-a-service model.

On the other hand, AVD is built for optimal flexibility. It offers a highly adaptable option for organizations with virtualization experience. Its usage-based pricing model is well suited for low-usage scenarios where customers can minimize costs by only paying for what they use. It also supports remote app streaming, multi-session virtual machines, and extensive customization.

Cloud PC – Windows 365	**Cloud VDI – AVD**
Optimized for experience	Optimized for flexibility
Windows 10 or Windows 11 personalized desktop	Windows 10, Windows 11, or Windows Server multi-session or personal desktops
Complete end-to-end Microsoft service	Remote app streaming
Windows 365 Boot and Switch	Not available
Requires Modern Desktop knowledge	Requires VDI and Azure infra knowledge

One-stop administration in Microsoft Intune (Enterprise edition)	Full control over configuration and management via Azure portal
Direct self-service model (Business edition)	Citrix and VMware support
Predictable per-user pricing	Pay for what you use

Table 1.1: Windows 365 and AVD differences

Components that Microsoft manages and the customer manages

Microsoft has done a great job with Windows 365 by simplifying the creation of Cloud PCs for users. Both the IT management and end user experience are very simple to learn and use. Getting started deploying Cloud PCs can be achieved in just a few clicks and the scalability is very powerful. Even though the Windows 365 service is almost a Plug and Play solution, there are a few things you as an organization must manage yourself; you still need to manage applications, settings, and security policies on your Windows 365 devices.

Depending on your domain and network configuration, you can either go full cloud with Entra ID (formally known as Azure AD) together with hosted networks or go for hybrid Entra ID. The table below helps you clarify the level of responsibility per service component. We also added AVD as a comparison on the right side to help reflect the differences.

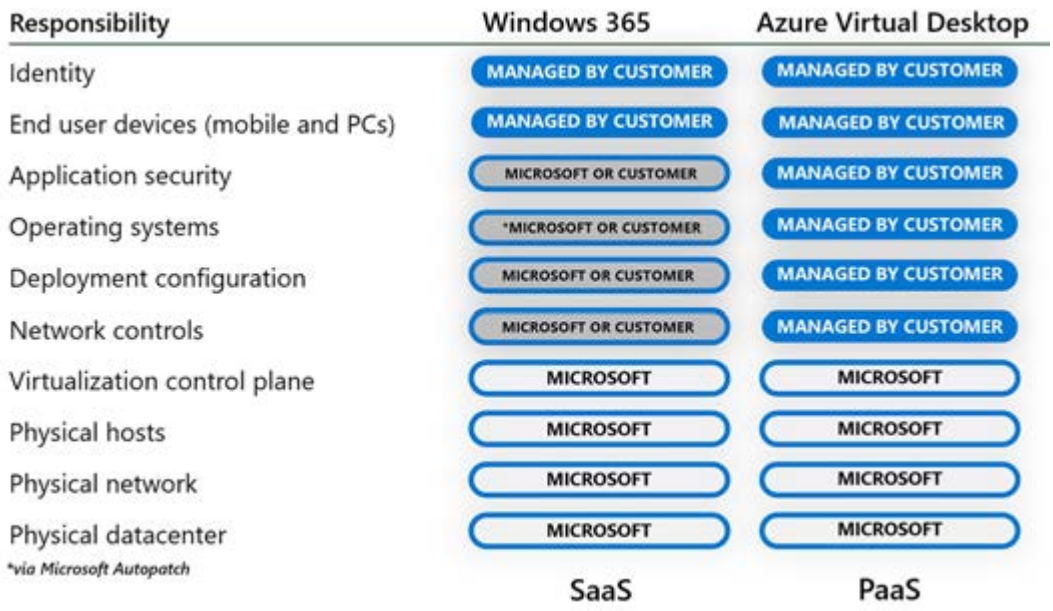


Figure 1.3: Service responsibilities

This concludes the section on Windows 365 and AVD. In the next section, we will cover Windows 11 Enterprise.

Windows 11

Windows 11 Enterprise is one of the primary components of your Microsoft 365 subscription. Windows 11 meets the needs of large and midsize organizations, providing users and organizations with the tools, services, and support to enhance their personal and organizational productivity.

Windows 11 also supports collaboration through Microsoft 365 apps, Microsoft Teams, Microsoft Whiteboard, and OneNote.

Windows 11 helps improve productivity by providing faster, safer ways to get work done across all your users' devices, by having some security feature defaults turned on, like Credential Guard. Windows 11 has hardware options ranging from Surface Hub to the new always-connected PCs. These options support users wherever they need or prefer to work. Users can move from one device to another with Continue on PC in Microsoft Edge or take notes directly on a web page with Microsoft Ink. Windows 11 also comes with a robust set of accessibility features, such as a narrator, word prediction, and eye control.

Windows 11 includes tools to help you customize device setup, manage all your devices, and control corporate identities, data, and apps on personal devices without impacting personal data. You can maximize security and productivity by staying current with Windows 11. The way to update Windows has changed completely. Major upgrades that previously happened every few years have now changed to updates that happen twice a year. Windows as a service, the model for Windows 11, provides the flexibility and control needed to manage and distribute updates using your current method or by using Microsoft's infrastructure.

Windows 11 protects, detects, and automatically responds to the most advanced malware and hacking threats while protecting user identities, devices, and your organization's information. Windows 11 investigates threats as they evolve and automates remediation to make response times faster, thanks to Intelligent Security Graph (which uses security intelligence, machine learning, and behavioral analytics). These security solutions are built-in and provide you with full security life cycle management for **Endpoint Protection** (**EP**) and **Endpoint Detection and Response** (**EDR**).

It also integrates with other Microsoft 365 services, which cover even the most complex multi-platform environments:

- **Threat protection**: Windows 11 threat protection includes next-generation malware and hacking defense to help protect against threats, including zero-day attacks. It provides a hardened platform that can help prevent encounters, isolate threats, and prevent the execution of malicious apps and content. Windows 11 can detect and respond to the most advanced threats and automatically remediate them.

- **Identity access**: Windows 11 protects user identities against pass-the-hash and pass-the-ticket attacks by helping you move to a world without passwords. **Windows Hello For Business** is a biometric authentication tool that strengthens authentication and helps guard against potential spoofing.
- **Information Protection**: Windows 11 makes it easy to protect data – whether that data is at rest or in use. Windows Information Protection helps protect sensitive information against leaks. When you combine Windows 11 with Microsoft Purview Information Protection and Microsoft 365, you get a sophisticated solution that meets the highest requirements for data loss prevention with minimal input.

Windows 11 is the next evolutionary phase of Windows; it is the most significant update to the Windows operating system since Windows 10. It offers a lot of innovations focused on enhancing end user productivity in a fresh experience that is flexible and fluid. Windows 11 is designed to support today's hybrid work environment and is intended to be the most secure, reliable, connected, and performant Windows operating system ever.

Windows 11 is built on the same foundation as Windows 10, so the investments you have made in tools for update and device management are carried forward. But Windows 11 has some new hardware requirements, such as the device needs to have a system firmware that runs **Unified Extensible Firmware Interface** (**UEFI**), Secure Boot, and a **Trusted Platform Module** (**TPM**) 2.0, which is also recommended on Windows 10 to enable many built-in Windows security features.

Windows 11 also provides unique hybrid remote work capabilities with Windows 365, such as the new Windows 365 Boot and Switch features that allow a user to connect to their Cloud PC from either the Windows 11 logon screen or via the Windows 11 Task View feature; more about that later in the book.

Windows 11 is Zero Trust ready and secure by design, with new built-in security technologies that will add protection from the chip to the cloud, while enabling productivity and new experiences. Key security features such as encryption, hardware-based isolation, and malware prevention are turned on by default. Going passwordless has also been made easier by simplifying the steps to deploy Windows Hello for Business.

Windows 11 Enterprise is secure by default, with advanced protection against modern security threats. It also includes virtualization-based security and hypervisor-protected code integrity, which is turned on by default (on newly installed Windows 11 devices).

To address the need for hybrid working in the market right now, location shouldn't matter. Addressing the new *how*, *when*, and *where* we work demands simplicity and security changes in the Windows operating system as well as the delivery of Windows in a simpler way – from the cloud with Windows 365:

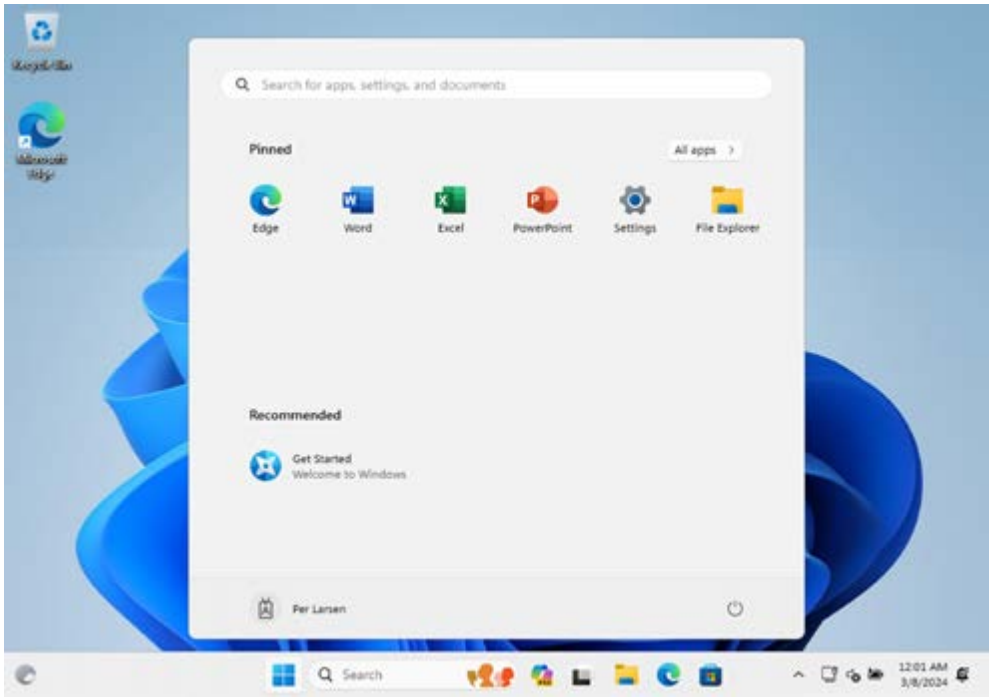


Figure 1.4: Windows 11

You can have a highly secure and consistent experience for users, with all the necessary IT controls, that delivers updates in a non-disruptive way, combined with a new, modern look and feel – that's the best way to describe what Windows 11 offers in a nutshell.

We will explain more about Windows 11 in *Chapter 6*, *Windows Deployment and Management*.

This concludes the section on Windows 11. In the next section, we will provide you with an overview of Windows Copilot.

Windows Copilot

Windows Copilot is your new assistant in Windows. It's an **AI assistant** integrated into **Windows 11** (**and Windows 10**). It aims to enhance productivity and creativity by providing real answers, inspiration, and solutions.

Here are the key features of Copilot:

1. **Assistance and focus:**
    - **Stay focused**: Copilot helps you stay on track while performing tasks. It adjusts PC settings and organizes windows using **Snap Assist**, saving you time and improving efficiency.

- **Task-oriented**: Whether you're adjusting settings or working online, Copilot assists you when needed.
- **State-of-the-art tools**: You can set Copilot aside when not required or launch it with a keystroke to access its powerful tools.

2. **Answers and inspiration**:
   - **Quick answers**: Copilot provides relevant answers promptly and allows follow-up questions.
   - **Creative spark**: Start your next project with ideas and information generated by Copilot. It can even create images from your concepts.
3. **Other AI-powered features in Windows 11**:
   - **Paint**: Enhanced tools for photo editing and art creation.
   - **Photos app**: Crop, erase, and adjust colors with ease.
   - **Photo Movie Editor**: AI in Snipping Tool simplifies text copying and redaction from screenshots.
   - **Clipchamp**: AI assists in editing footage for faster publishing.
   - **Smart App Control**: Predicts safe app downloads.
   - **Windows Security**: AI-powered tools for figuring things out and quick searches.

Windows Copilot combines seamlessly with **Bing Chat** and **ChatGPT plugins**, allowing you to stay in your flow without switching between apps. It's like having a smart, helpful companion right within your Windows environment!



Figure 1.5: Windows Copilot with Bing Chat

This concludes the section on Windows Copilot. In the next section, we will give you an overview of Security Copilot.

Security Copilot

Security Copilot, a novel tool powered by OpenAI GPT, is offered as a cloud-based service to enhance the security of your Microsoft Security cloud services, including Microsoft Intune.

Security Copilot is designed to work with all Microsoft Security services. This encompasses Security Operations, Device Management, Identity Management, Data Protection and Compliance, and Cloud Security. In this book, we will concentrate on the application of Security Copilot for Device Management via Microsoft Intune. Learn more about it in *Chapter 12*, *Copilot/AI*!

Intune Copilot

Intune Copilot is a new OpenAI GPT-based tool offered as a cloud-based service to bolster the security of your Microsoft Security cloud services. Microsoft Copilot addresses this security-related query and illustrates how to utilize this innovative AI tool. It employs real-world examples to delve into how Security Copilot aims to disrupt conventional methods across diverse cybersecurity domains. You will learn more about Security Copilot in *Chapter 11*.

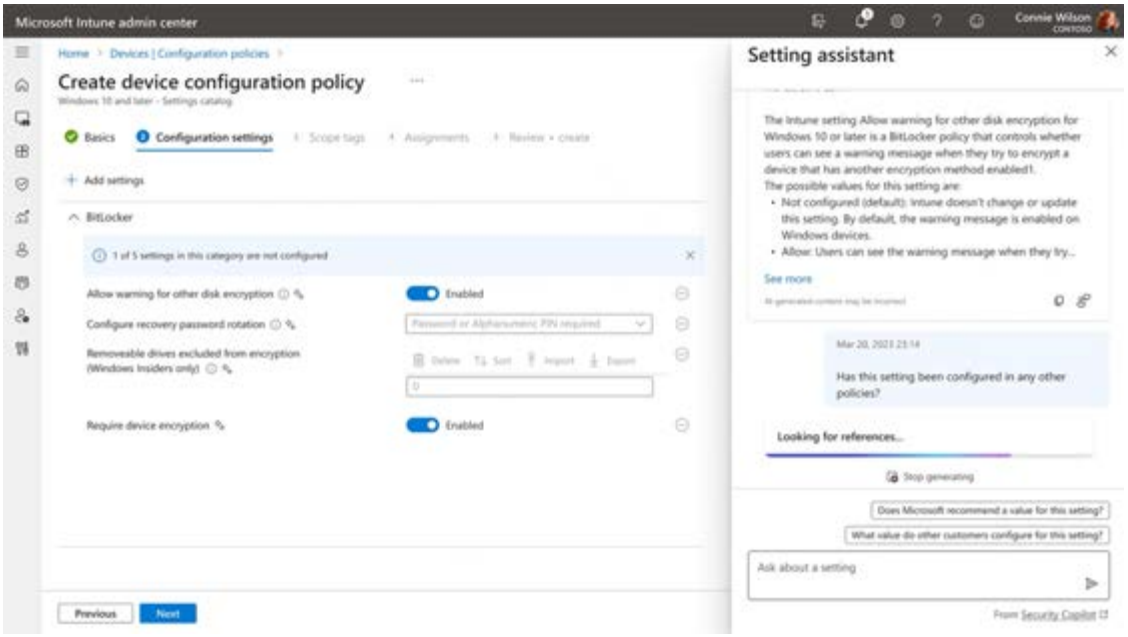


Figure 1.6: Security Copilot

This concludes the section on Copilot. In the next section, we will give you an overview of Productivity Score.

Productivity Score

The journey to digital transformation is supported by Productivity Score, which provides insights into how your organization uses Microsoft 365 and the technology experiences that support it. Your organization's score reflects the effectiveness of your people's work and technology and can be compared to benchmarks from organizations similar in size to yours.

Productivity Score provides the following:

- Measurements that provide a clear picture of your progress on your digital transformation path
- Data-driven insights that highlight opportunities to boost productivity and satisfaction within your organization
- Steps you can implement to ensure efficient utilization of Microsoft 365 products in your organization

The following Productivity Score screenshot shows you the level of insights you get based on scoring metrics in the Microsoft 365 admin portal:

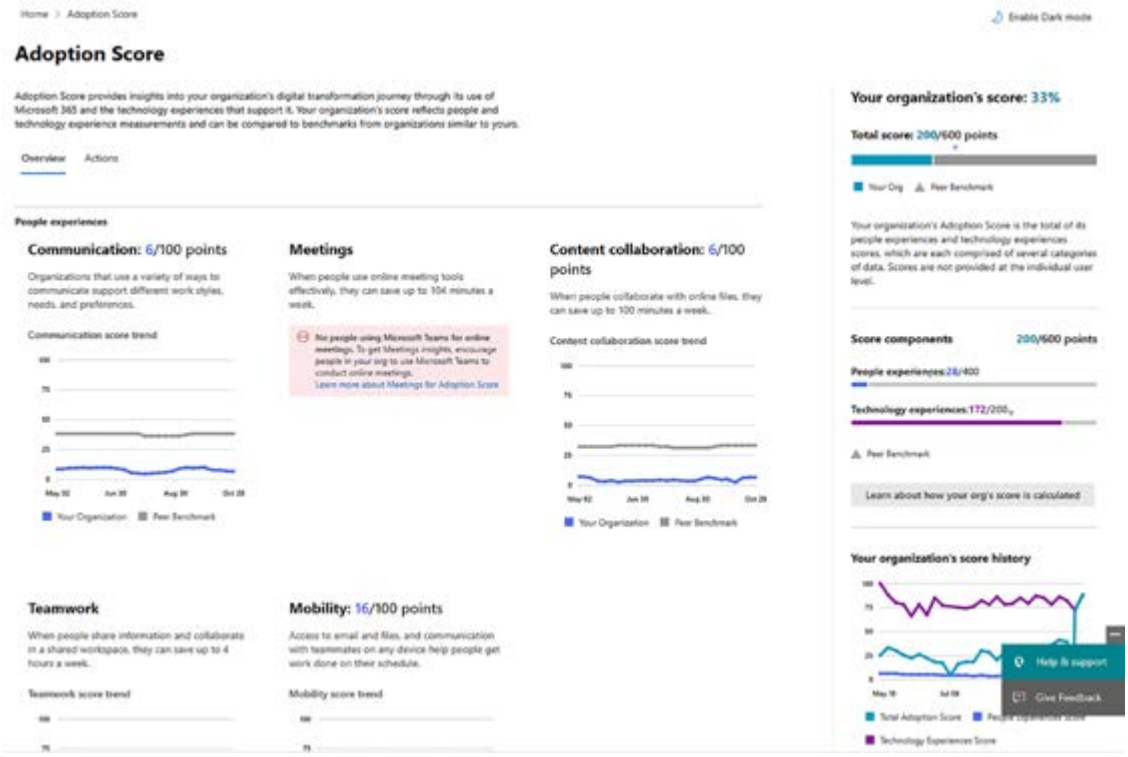


Figure 1.7: Adoption Score

Your Productivity Score is calculated from the aggregate scores of your people and technology experiences categories. Each category carries equal weight, contributing to a total of 100 points. The maximum achievable Productivity Score is 800.

Adoption Score incorporates Endpoint analytics as well. Your Endpoint analytics score evaluates the caliber of the technology experience you're providing for your users and suggests ways to enhance it.

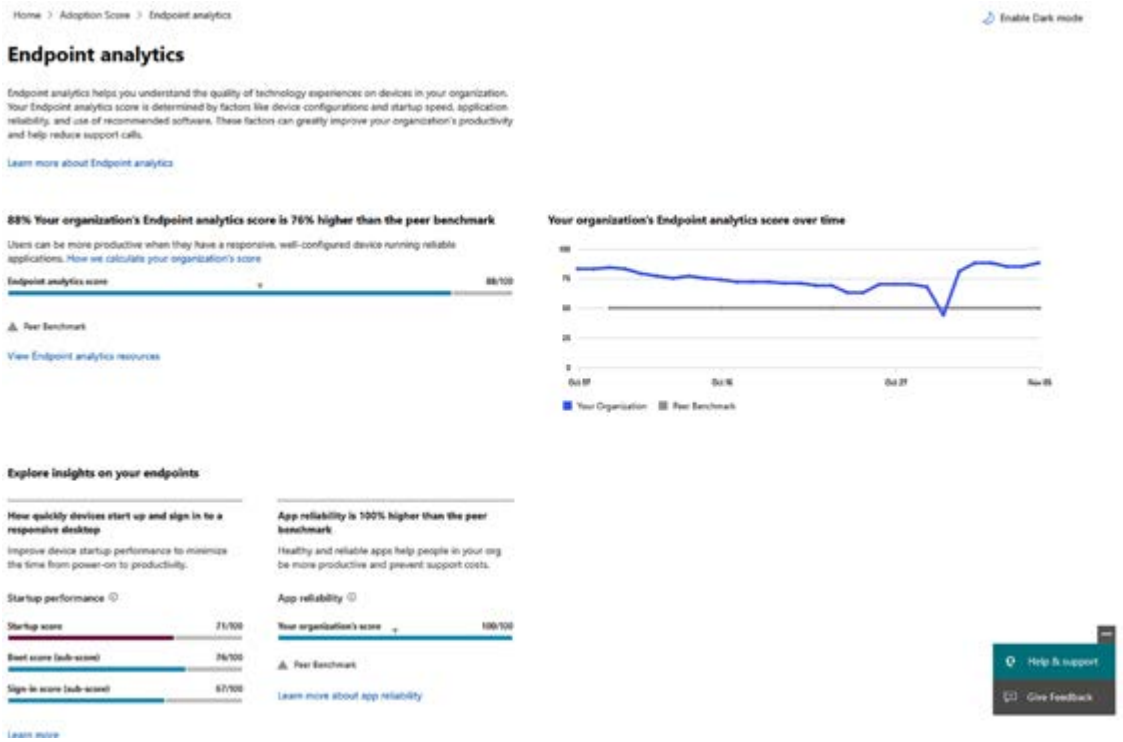


Figure 1.8: Endpoint analytics

This concludes the section on Productivity Score with the integration of Endpoint analytics, which you will get an overview of in the next section.

Endpoint analytics

Endpoint analytics is a service in your Intune tenant that provides you with data on the performance of your Windows devices that are managed by Microsoft Intune; this data is part of Productivity Score. Everything that is collected comes from measurements of how your business is working. For example, Endpoint analytics gives you insights into the boot time of your physical device, logon duration, and application startup time.

The insights enable IT admins to reduce support costs by adding capabilities to proactively solve issues in their environment. This can all happen automatically without any involvement of the IT admin:

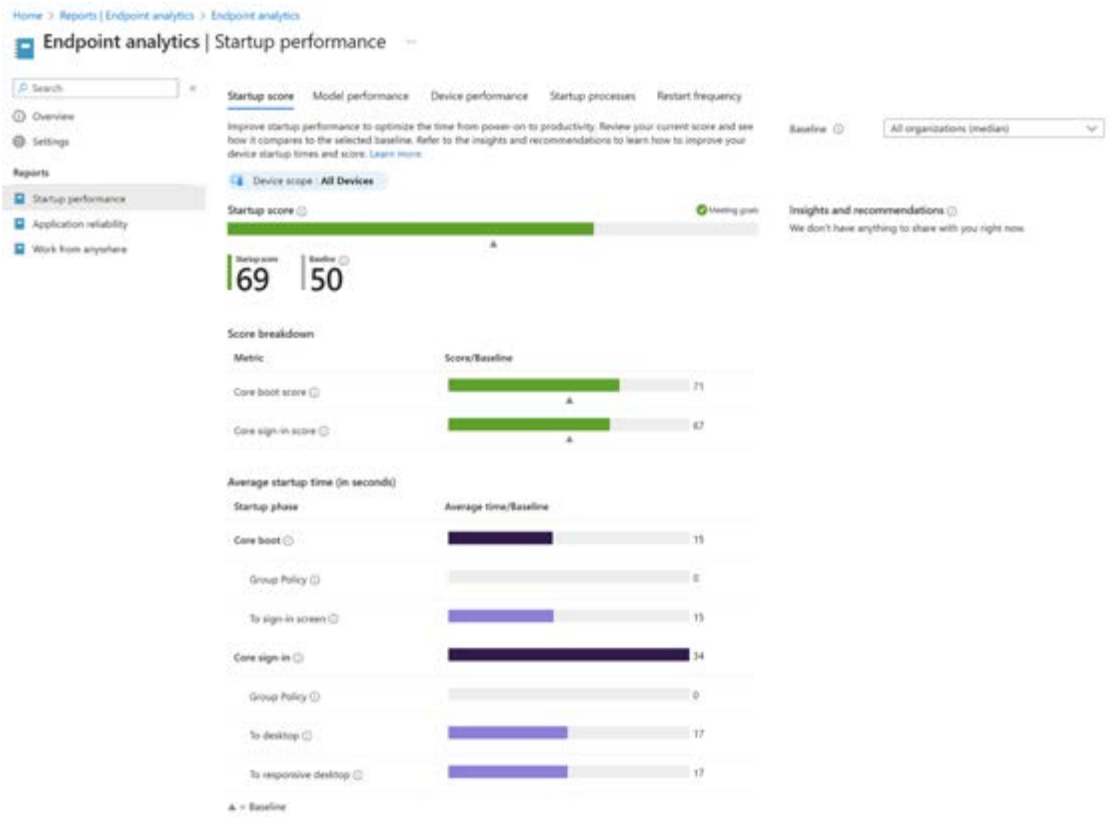


Figure 1.9: Endpoint analytics

Your end-to-end experience can be dramatically improved by Endpoint analytics and the benefits it brings. Another huge benefit is that all service costs are included; unlike with Azure Monitor, there is no need to pay for storage retention!

This concludes the overview section on Endpoint analytics. In the next section, we will give you an overview of Microsoft 365 apps.

Microsoft 365 Apps (for Enterprise)

In the long list of Microsoft 365 Apps for Enterprise, you will find all the productivity applications:

- Word
- Excel
- PowerPoint
- Forms
- OneNote
- Sway
- Planner
- Loop
- List
- Power Apps
- Stream
- OneDrive
- Teams (limitation within EEA)

Microsoft 365 Apps is both a web-based version of Office and also a click-to-run installation locally on your user's device, both on Windows and macOS. You can use the Office applications that come with Microsoft 365 Apps with the on-premises or online versions of Exchange, SharePoint, or Teams.

The new subscription structure for Microsoft 365 in Europe per October 1, 2023 for the **European Economic Area** (**EEA**) and Switzerland means that Microsoft Teams will no longer be included in Microsoft 365 Apps, but it can be purchased separately.

You can install Microsoft 365 Apps from a network share or directly from the internet. After it's installed, you don't have to be connected to the internet to use it. However, you'll need to connect at least once every 30 days to ensure that your license is still active.

Microsoft 365 Apps is updated either monthly or semi-annually with new features, security updates, and other quality updates from Microsoft. You can choose which frequency works best for your organization by selecting specific update channels.

OneDrive for Business (part of Microsoft 365 Apps)

Microsoft OneDrive is an enterprise file-sharing service that allows you to easily store and securely access your files from all your physical, virtual, and mobile devices. You can work together with people from any location, regardless of whether they're inside or outside your organization, while also exploiting comprehensive security capabilities; for example, only allowing data sharing based on several security baseline conditions. All of your data that is stored in OneDrive's cloud service is protected using advanced encryption while in transit and at rest in data centers.

OneDrive enhances collaboration capabilities within Microsoft 365 Apps by connecting you to your personal and shared files in Microsoft 365. With OneDrive on the web, desktop, or mobile, you can access all your personal files and any files shared with you by other people or teams, including files from Microsoft Teams and SharePoint.

Another great feature is OneDrive cloud backup – also known as OneDrive folder backup (previously Known Folder Move). This service automatically syncs your `Desktop`, `Documents`, and `Pictures` folders on your physical or virtual endpoints to your OneDrive cloud storage. Your files and folders stay protected and are available from any device!

This concludes the section on Microsoft 365 apps. In the next section, we will provide you with an overview of Microsoft Teams.

Microsoft Teams

Microsoft Teams is a unified communications collaboration tool that brings different services together to modernize the way you work with colleagues and external businesses. Teams allows you to implement a chat-based workspace as part of your Windows 11 physical and Cloud PCs with local experiences but also as a mobile app on various platforms, which helps you stay up to date both in the office and on the go.

Teams keeps your team in sync by sharing OneDrive and SharePoint documents, insights, and status updates while being able to manage important projects and easily locate people – from anywhere and on any device!

With Microsoft Teams, you can do the following:

- **Engage in chats, meetings, and calls**: Conduct audio, video, and web conferences, and engage in conversations with anyone within or outside your organization.
- **Collaborate using Microsoft 365 apps**: Teams simplifies teamwork by enabling users to co-create and share files with popular Microsoft 365 apps, ranging from Microsoft Word to Microsoft Power BI.
- **Personalize your workspace and enhance productivity**: With Teams, you can incorporate apps from Microsoft and third-party services to cater to your organization's specific requirements.
- **Stay connected across devices**: Teams and Teams devices seamlessly integrate for smart meeting and calling experiences. Choose the right devices for your needs and bring your innovative ideas to fruition.

Below, you can find the latest new Microsoft Teams client with many performance and resource utilization updates benefiting the user experience and cost for Cloud PCs. There's also great news to share about using Microsoft Teams together with Windows 365. We've improved the plugin experience, eliminating the need for updates to this designated plugin, as everything now happens in the background!

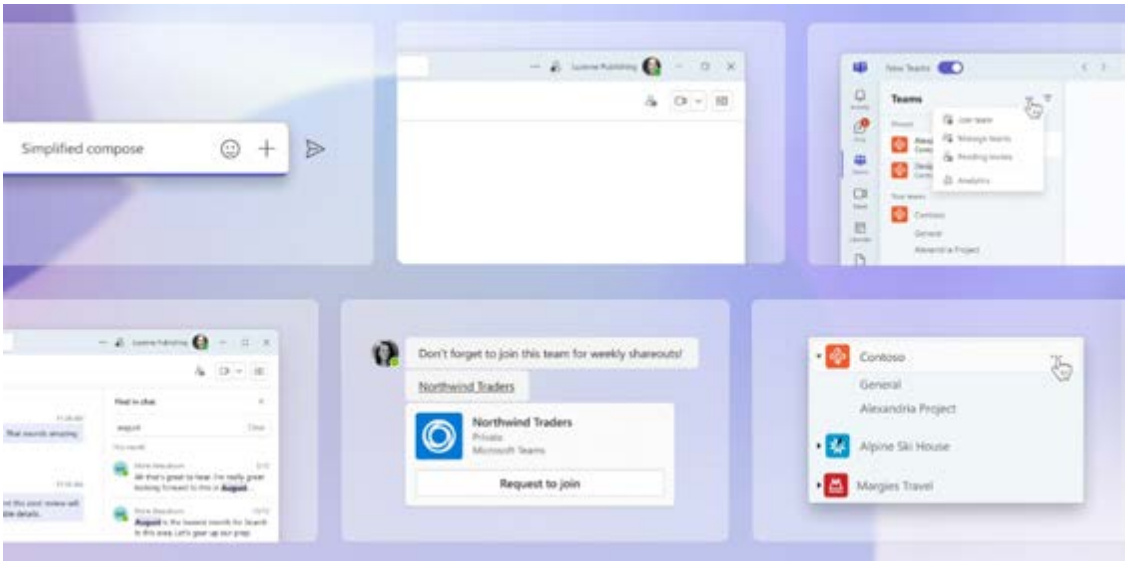


Figure 1.10: Microsoft Teams Client

This concludes the section on Teams. In the next section, we will give you an overview of Microsoft Edge.

Microsoft Edge

Microsoft Edge has been around for a while (first released in 2015) and is the next modern iteration of Internet Explorer. The new Microsoft Edge is built on the open source project "The Chromium Project," which is also the same as Google Chrome. Microsoft Edge is also cross-platform, so the end user can get the same enterprise browser experience no matter what device they are using.

Microsoft Edge has proven to be very fast and uses less memory than Google Chrome. Its alignment with other Microsoft services such as Microsoft Intune to set policies, as well as the cross-platform support for the app to sync data such as personal history and favorites settings, has been well received. This has resulted in Edge being the default browser for Windows 10 and Windows 11 to date.

Microsoft Edge is available on Windows, macOS, iOS, Android, and Linux. You can choose what device you want to use with the same native Edge experience across different platforms.

Edge for Business is a specialized work-oriented experience provided by Microsoft Edge. It's an advanced version of Microsoft Edge, designed to help organizations enhance productivity and security while maintaining a clear distinction between professional and personal browsing.

Some of the features of Edge for Business are:

- You can sign in with your work account and get access to a separate browser window with a briefcase icon and a **Work** label next to your profile image.
- You can also sign in with a personal account and launch a personal browser window that keeps your favorites, passwords, and history separate from your work browser window.
- Edge for Business will automatically recognize sites that require your work account and open them in the work browser window, and vice versa for popular non-work sites.
- Edge for Business has new native enterprise-grade security, productivity, manageability, and AI built in as features. Passwords, favorites, and data are not shared between the work profile and personal profile in Edge.
- **Mobile Application Management** (**MAM**) for Edge is a feature that allows you to manage and protect the Microsoft Edge browser on Windows devices without enrolling them in Intune – also known as BYOD. You can use MAM for Edge to configure app settings, apply app protection policies, and enforce conditional access rules.

This concludes the section on Microsoft Edge. In the next section, we will give an overview of Universal Print.

Universal Print

You may recall, or perhaps still utilize, the following process: setting up a Windows Server environment, incorporating the print server role, and then adding your printers and specific drivers to the server. It's not exactly cutting-edge or efficient, is it? Universal Print provides the same features and more, while also doing away with the need for on-site infrastructure. It allows you to control printers directly via a centralized portal in Microsoft Azure. No more installing (and maintaining) printer drivers on devices or golden images. As an added perk, everything is compatible with Entra ID. This means users can employ the same credentials they use for other Microsoft services, whether they're logging on to a physical desktop or a cloud-based virtual desktop.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is the business-oriented variant of Microsoft Defender, which comes as a standard feature in Windows 11 Enterprise. It's a cloud-based security solution aimed at assisting corporate networks in averting, identifying, examining, and reacting to sophisticated threats. The service is integrated end-to-end into the Microsoft Intune console and therefore aligns easily with other compliance and security settings and roles as part of your security baselines.

One of the great features of integrating Defender within Microsoft Intune is that after your organization onboards a device using the configuration package, you will never have to do it again. All your physical and/or cloud PCs will be secured out of the box:

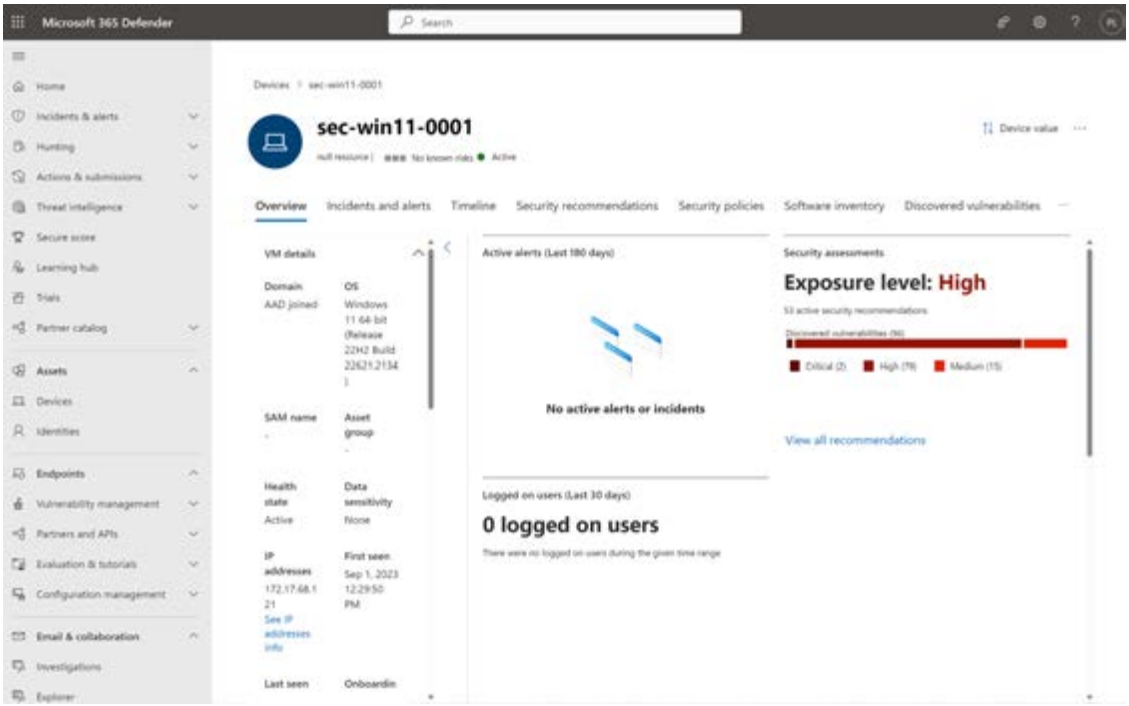


Figure 1.11: Defender for Endpoint security center

The Defender for Endpoint onboarding process in Intune is very simple and is something we will cover in *Chapter 13*.

This concludes the overview section on Defender for Endpoint. In the next section, we will give a short overview of Exchange Online.

Exchange Online

Exchange Online is a messaging and collaboration platform for your email, calendar, contact info, and tasks. You can access all of this with Microsoft Outlook, Outlook on the web, or Outlook Mobile. You can access Exchange Online on most devices, including Android, iOS, and Windows devices with internet access.

SharePoint Online

SharePoint Online is the cloud-based version of Microsoft SharePoint Server, designed to facilitate collaboration and communication through team- or communication-centric sites. It's accessible to internal users who have a valid Microsoft 365 or SharePoint Online license. These users can share files or folders with individuals inside or outside their organization, with external sharing controlled by site administrators.

With SharePoint Online, users can:

- Construct sites, pages, document libraries, and lists.
- Incorporate web parts to personalize their pages.
- Disseminate crucial visuals, updates, and news within a team.
- Search for and locate sites, files, individuals, and news throughout their organization.
- Oversee their business operations using flows, forms, and lists.
- Synchronize and save their files in the cloud, allowing secure access for anyone.
- Stay updated with news on the move via the SharePoint mobile app.

Summary

In this chapter, you learned about different Microsoft 365 services you might use in your day job or as part of your journey to using Microsoft Intune to simplify the management overhead of your environment. What you didn't learn is that some of these services cost more on top of the existing Intune subscription.

This chapter is mainly intended to provide context for the later chapters in the book; we are now switching gears and taking you on the journey of unified endpoint management with Microsoft Intune.

Questions

1. What are the main benefits of using Microsoft Intune?
    a. Microsoft Intune ensures that an organization no longer needs credentials to access and share company data.
    b. Microsoft Intune prevents remote devices and apps from accessing an organization's resources.
    c. Microsoft Intune helps keep an organization's cloud and on-premises devices, apps, and data secure.
2. On what Windows version are Windows 365 Boot and Windows 365 Switch available?
    a. Windows 10
    b. Windows 11

Answers

1. (C)
2. (B)

Further reading

If you want to learn more about Microsoft Intune after reading this chapter, please use the following free online resources:

- *Microsoft Intune fundamentals*: `https://docs.microsoft.com/en-us/learn/paths/endpoint-manager-fundamentals/`
- *Windows 365 official product documentation*: The official Microsoft documentation for Windows 365 Enterprise and Windows 365 Business (`https://learn.microsoft.com/windows-365`)
- *Introduction to Microsoft Intune*: `https://docs.microsoft.com/en-us/learn/modules/intro-to-endpoint-manager/`

Get This Book's PDF Version and Exclusive Extras

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

Note: *Keep your invoice handy. Purchases made directly from Packt don't require one.*

UNLOCK NOW

2

Cloud-Native Endpoints

The concept of cloud-native endpoints refers to devices that can be provisioned anywhere, cloud-native endpoints are devices that can be provisioned from anywhere and receive applications, policies, and maintenance updates throughout their lifetime from the cloud. You will learn about the concept of cloud-native endpoints and Zero Trust with Microsoft Intune, along with its history and architectural concepts, to get a clear understanding of how all devices – physical, virtual, and mobile – come together in a single management console.

In this chapter, we'll go through the following topics:

- What are cloud-native endpoints?
- Microsoft Intune
- Exploring Windows 11 Enterprise in detail
- Windows Autopatch
- **Bring Your Own Device** (**BYOD**)
- What is Zero Trust?
- Windows 365 for non-managed endpoints

Paths to cloud native

Modern management is a comprehensive approach to managing Windows devices in a consistent and unified way without compromising the security of endpoints. It involves the execution of strategies that equip IT to evolve the modern workplace into a space that is cherished by users, appreciated by IT, and trusted universally. The essence of modern management lies in cloud intelligence, which facilitates streamlined, contemporary management through cloud-based device management solutions like Microsoft 365.

The modern desktop is the state-of-the-art productivity platform for the information worker. Microsoft 365 apps and Windows 11 are the core components of the modern desktop along with the latest security baselines for Windows 11 and Microsoft Defender for Endpoint.

Since the first Windows 10 release back in 2015, Microsoft included the **Mobile Device Management** (**MDM**) stack natively built in, and along with that many companies have explored new management options, with one of these being advancements in cloud technology. **BYOD** trends have made the move toward modern management more compelling for many organizations, not only for mobile devices running iOS and Android but also for physical and cloud-based Windows PCs.

Modern management is a new approach to managing Windows 11 devices, in the same way as mobile devices are managed by **Enterprise Mobility Management** (**EMM**) solutions. The modern management approach allows your organization to simplify deployment and management, improve security, provide better end user experiences, and lower costs for your Windows devices.

There are three waves to unified endpoint management:

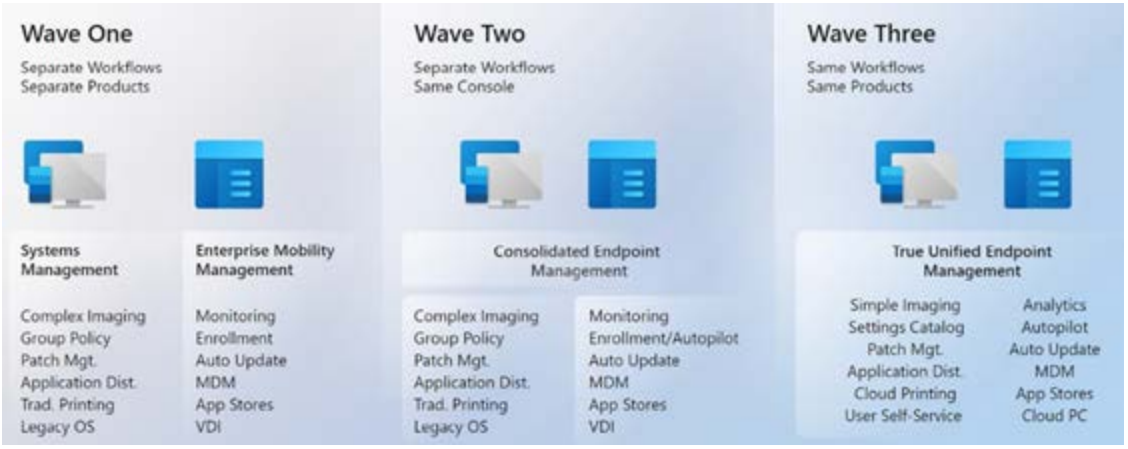


Figure 2.1: Unified endpoint management phases

Modern management allows you to administer a variety of Windows devices, ranging from physical and cloud PCs to HoloLens, Microsoft Teams Rooms systems, and Surface Hub. This includes both corporate-owned and personal devices, as well as mobile devices, all through a unified management platform, Microsoft Intune.

Microsoft Intune

What is unified endpoint management and how does this look through the concept of **Microsoft Intune**? The following high-level architecture drawing (*Figure 2.2*) explains how everything within Microsoft Intune comes together in one unified endpoint management experience.

There is one console for your physical and cloud PCs via **Windows 365** endpoints and mobile devices. This is the only place where they can be managed in a unified way. Also, the Intune company portal can deploy apps from Configuration Manager, Intune, Windows 365, Azure Virtual Desktop, and Microsoft Entra ID – one end user experience for all apps!

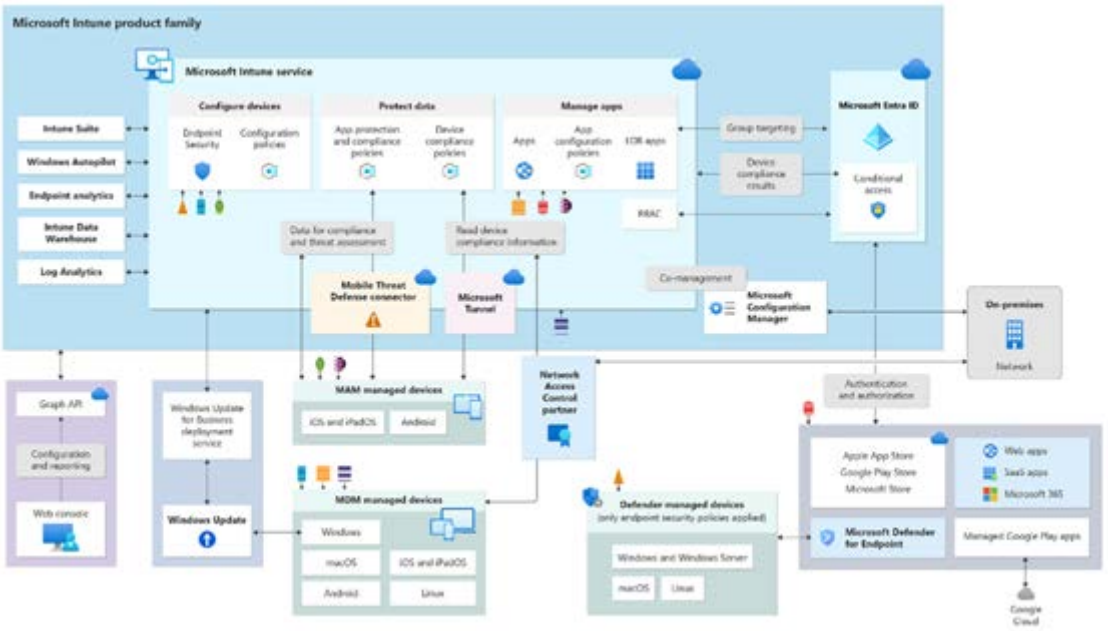


Figure 2.2: Microsoft Intune architecture diagram

The diagram of the Microsoft Intune architecture illustrates the three stages of the cloud management journey using Configuration Manager and Intune as a single, unified endpoint management solution:

1. Tenant attach
2. Co-management workloads
3. Cloud-native management

All new Windows devices should go directly to the cloud with **Microsoft Entra ID** with automatic enrollment into Intune. This leverages Windows Autopilot for the best onboarding experience for IT and end users. If your organization already has a Configuration Manager environment with lots of applications that you are deploying to your on-premises managed devices, you can leverage the same application delivery method by using the built-in option **Co-management settings** in Intune to provide a coherent end user onboarding experiences for new devices.

We recommend waiting for a reason to go cloud native. As an example, you can move to Entra joined devices during a hardware refresh or device troubleshooting scenario when there's a new (or reset) instance of Windows. Using this approach, you minimize user disruption and streamline the conversion process to Entra ID Join. Remember, there's no Microsoft-supported process or path to convert an existing device from **Hybrid Azure Active Directory Join** (**HAADJ**) to **Azure Active Directory Join** (**AADJ**) without a Windows device reset. This would involve user downtime and loss of productivity.

You can proactively reset existing devices to move to Entra ID Joined. This approach can be more disruptive to end users and requires more planning and testing. But, you can use this approach if you have an end user scenario where it makes sense to reset devices or if you have a strong business case to move to Entra ID Joined.

For pre-existing devices, begin utilizing tenant-attach features that offer the most adaptable route for Configuration Manager users to start reaping the benefits of the cloud without necessarily registering their Windows clients with Intune. Link the Configuration Manager environment to the cloud and instantly gain access to a range of remote actions and endpoint analytics. If your organization is ready for the next step, you can start onboarding Windows devices into a co-management state, which means managing Windows clients using both Configuration Manager and Intune. Leverage the best of both worlds by moving one workload to the cloud at a time.

Intune admin center portal

The Microsoft Intune admin center portal serves as your comprehensive, single-point admin platform for formulating policies and managing your devices. It empowers IT administrators to incorporate other essential device management services, such as groups, security baselines and settings, Conditional Access, analytics tools, and reporting.

Microsoft Intune is a fully cloud-based MDM and MAM service for your applications and devices. It allows you to regulate features and settings on Android, Android Enterprise, iOS/iPadOS, macOS, and Windows devices. It also integrates with other services, including Entra ID, and mobile threat defense mechanisms.

In the Microsoft Intune portal, you can create compliance policies and check the compliance status of targeted devices. The device compliance policy marks the device as compliant or non-compliant. If you have enabled Conditional Access in your Microsoft 365 cloud environment, you can leverage compliance status from Intune to allow or block access to corporate data.

Microsoft 365 admin center portal

In the Microsoft 365 admin center portal (`https://admin.microsoft.com`), you can manage and administer all your Microsoft 365 cloud services. The most common task that you perform in this portal is to purchase and assign licenses for your Microsoft services.

Here's a full list of what you can do via the Microsoft 365 admin center:

Menu	What it's for
Home	This is the landing page in the admin center. You'll see where to manage users, billing, service health, and reports.
Users	Create and manage users in your organization, like employees or students. You can also set their permission level or reset their passwords.
Groups	Create and manage groups in your organization, such as a Microsoft 365 group, distribution group, security group, or shared mailbox.
Resources	Create and manage resources, like a SharePoint site collection.
Billing	View, purchase, or cancel subscriptions for your organization. View past billing statements or view the number of assigned licenses to individual users.

Support	View existing service requests or create new ones.
Settings	Manage global settings for apps like email, sites, and Microsoft 365. Change your password policy and expiration date. Add and update domain names like contoso.com. Change your organization profile and release preferences. And choose whether partners can access your admin center.
Setup	Manage existing domains, turn on and manage multi-factor authentication, manage admin access, migrate user mailboxes to Microsoft 365, manage feature updates, and help users install their Microsoft 365 apps.
Reports	See at a glance how your organization is using Microsoft 365 with detailed reports on email use, Microsoft 365 activations, and more.

Table 2.1: Microsoft 365 admin center portal

Let's talk more about how Microsoft Intune helps OEM partners.

Intune Partner portals

In the Microsoft Intune admin center, under **Devices | Partner portal**, you are able to access different hardware partner portals:

- **Surface Management Portal**
- **HP Connect**



Figure 2.3: Microsoft Intune Partner portal

Surface Management Portal

The Surface Management Portal is already configured within your Intune tenant and will show your devices as soon as you have enrolled them into Intune.

If you do not have any Surface devices in your environment that are enrolled in Microsoft Intune, it will just show this:



Figure 2.4: Surface Management Portal – No Surface devices found

The Surface Management Portal is a unified platform that enables IT administrators to manage and monitor all Microsoft Surface devices on a large scale within Microsoft Intune. Integrated into the Microsoft Intune admin center, it offers a comprehensive environment for complete visibility of both corporate and user-owned Surface devices.

The portal lets you quickly see any issues that need prompt attention before they hit your helpdesk. You can get insights into device compliance, support activity, and warranty coverage. Quickly see the status of each device, which ones are still in warranty or expiring soon, and the status of active support requests with your hardware providers.

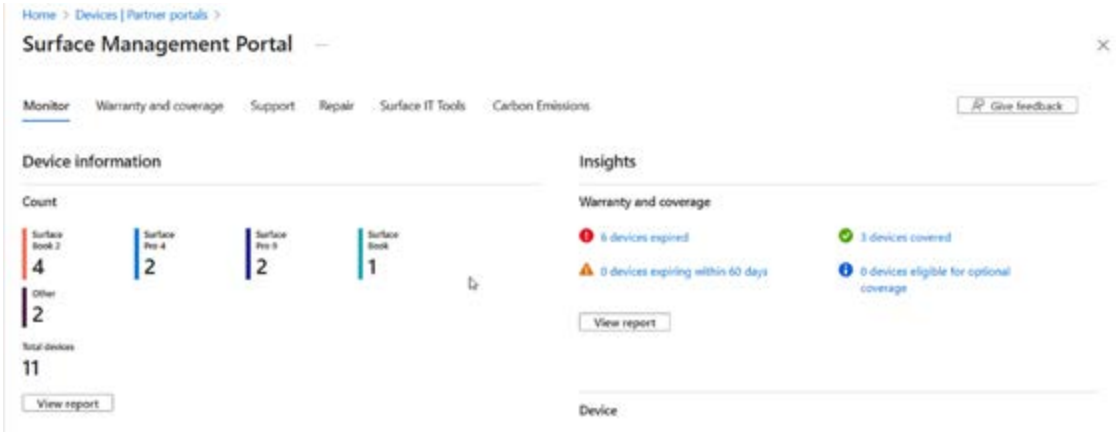


Figure 2.5: Microsoft Surface Management Portal

HP Connect

HP Connect is a cloud application designed to ease the management of UEFI BIOS on supported HP systems. HP Connect has a framework for developing BIOS management policies that are published to Microsoft Intune. HP Connect creates the policies and Intune executes them as remediation scripts. HP Connect requires a valid Microsoft Entra ID subscription and Microsoft Intune as the registered MDM. HP Connect interfaces directly with a customer's Entra ID tenant for access to device groups and publishing BIOS policies as a cloud application.



Figure 2.6: HP Connect

You need to click **Get started** to start the integration process. Sign in with an admin user who has the correct role-based access in Entra ID to consent to a new Entra ID app in your organization.

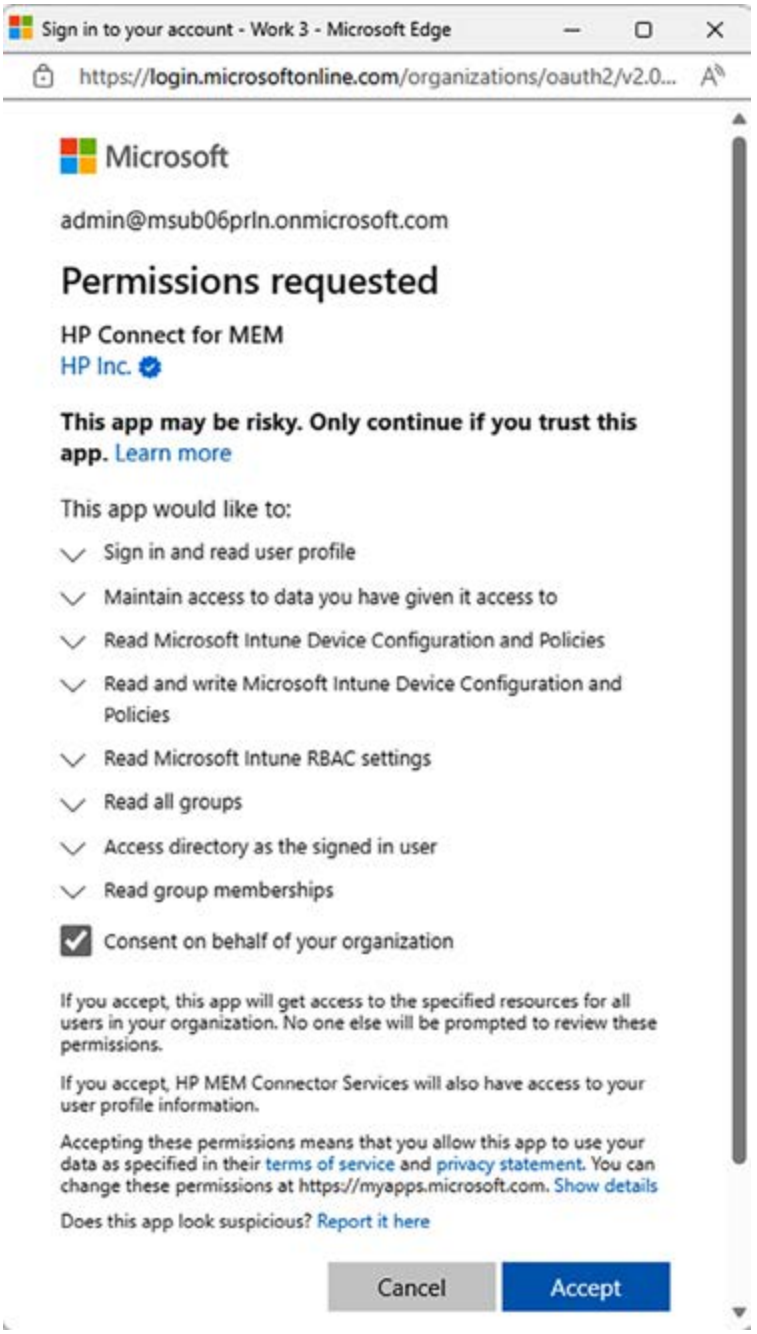


Figure 2.7: HP Connect

You need to accept the terms and conditions from HP to continue the integration.

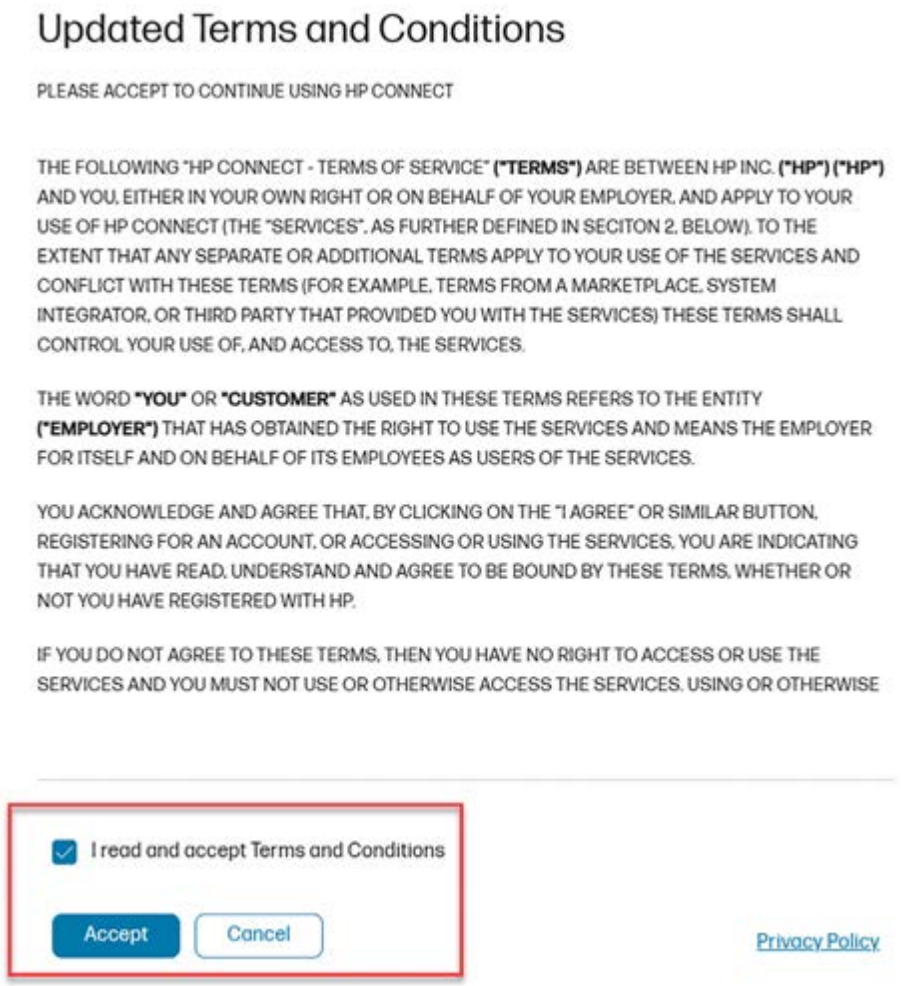


Figure 2.8: HP Connect terms and conditions

HP Connect is a cloud-based application engineered to simplify the administration of UEFI BIOS on compatible HP commercial systems. It possesses a structure for formulating BIOS management policies concerning authentication, updates, and settings, which are disseminated to Microsoft Intune device groups. While HP Connect is responsible for policy creation, Intune carries out these policies as proactive compliance rectifications.

In other words, HP Connect for Intune enables IT administrators to manage the BIOS configuration of HP commercial systems using Microsoft Intune. It simplifies the process of deploying firmware updates and managing BIOS configuration and ensures that the devices are compliant with the organization's hardware security policies.

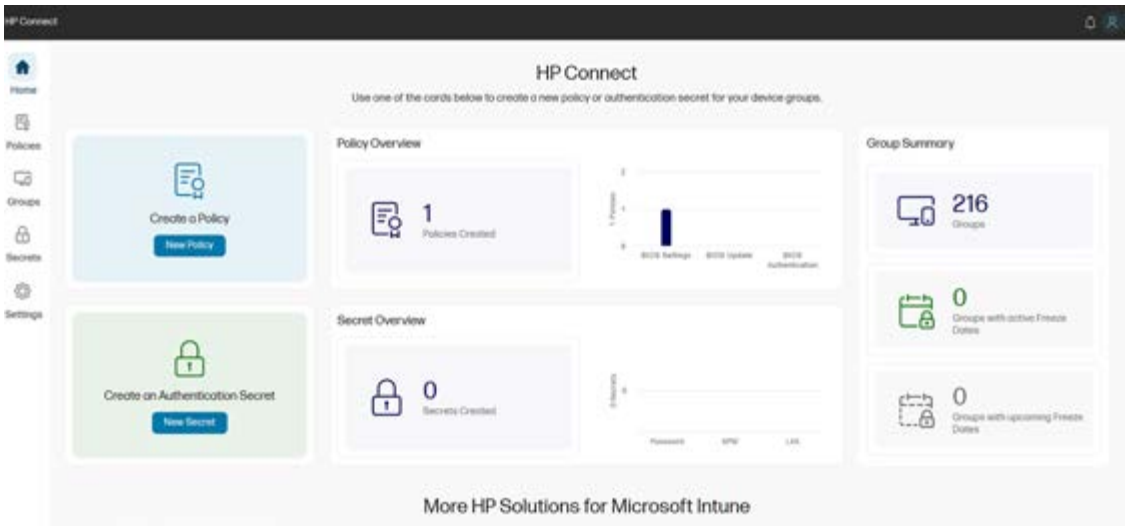


Figure 2.9: HP Connect for Microsoft Intune

You can create a policy in HP Connect that deploys a specific HP EliteBook BIOS version. Use the sample screenshot below as a pointer to get started with your HP EliteBook BIOS updates.

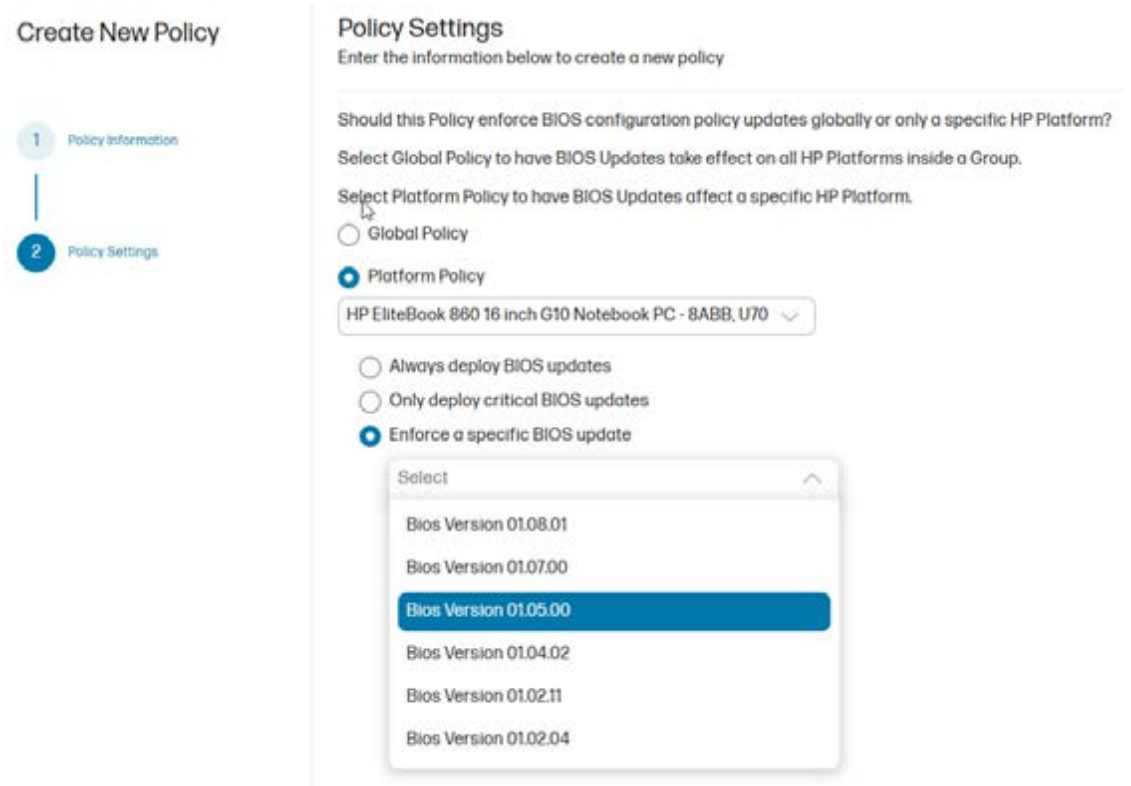


Figure 2.10: HP Connect policy for specific BIOS versions

There are three types of BIOS update policies supported by HP Connect:

- **Always deploy BIOS updates:** When implemented on a set of supported platforms, Intune will employ the policy as a compliance measure to track and update each device in the chosen group whenever a BIOS update is launched that corresponds to a device within the group.
- **Only deploy critical BIOS updates:** This policy will apply for a new BIOS release if it is marked as "Critical" by HP to every matched device in the selected group.
- **Enforce a specific BIOS update:** This policy will apply a BIOS update to a matching device in a device group based on a defined criteria/rule. The policy is applied to the specified platform only.

Policy settings created in HP Connect for Intune will show up as remediation scripts inside Microsoft Intune.

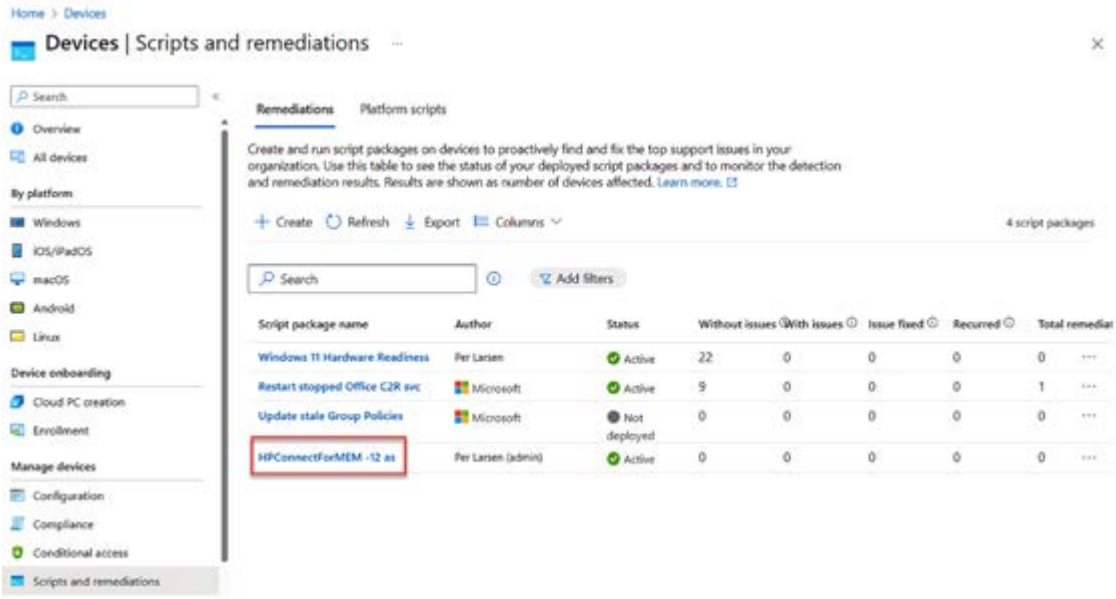


Figure 2.11: HP Connect remediation scripts

Learn more at `https://connect.admin.hp.com/static/HPConnectUserGuide.pdf`.

This concludes the section on the Intune Partner portal. In the next section, we will cover Windows 365.

Windows 365

Windows 365 is the ideal solution if you're seeking a streamlined approach to operating your Windows PCs in the cloud. It reduces costs and simplifies your environment as you deploy and manage virtual endpoints in Microsoft Intune, with no need for extra **Virtual Desktop Infrastructure** (**VDI**) expertise or resources.

Windows 365 is a comprehensive SaaS service that securely provides a personalized Windows desktop, apps, settings, and content from the Microsoft cloud to any device, marking a new era in PC accessibility.

Microsoft's unique offering, a cloud PC, coexists alongside traditional physical PCs, providing an end-to-end solution with unified management through Microsoft Intune. This means that it's an end-to-end solution where customers can leverage the power from a computer from the cloud, with the same management tools to manage their physical and cloud PCs (Microsoft Intune admin portal).



Figure 2.12: AVD and cloud PC overview

More information about Windows 365 will follow later in this book. In the next section, we will cover Microsoft Entra ID.

Microsoft Entra ID

Microsoft Entra ID serves as the identity provider and access management service for Microsoft Intune; this means that users and groups always are managed in Entra. Microsoft Intune then manages your MDM-enrolled devices and assigns apps and configurations to groups of users and/or devices, enabling advanced Conditional Access capabilities such as **Multi-Factor Authentication** (**MFA**) and compliance-based filtering. With Entra ID Premium, you can incorporate several additional features to safeguard devices, apps, and data, including dynamic groups, automatic enrollment, and Conditional Access.

Configuration Manager is an on-premises management solution for managing desktops, servers, and laptops that are either network based or internet based. It can be cloud enabled to integrate with Intune, also referred to as co-management or tenant attached, Entra ID, Microsoft Defender for Endpoint, and other cloud services. Configuration Manager can be used to deploy apps, software updates, and **Operating Systems** (**OSs**). It also allows for compliance monitoring, real-time client querying and action, and much more.

Even as an on-premises product, Configuration Manager has a biannual update cycle with a built-in semi-automatic update process tool, eliminating the need for you to search for, download, and install updates for your Configuration Manager.

This concludes the overview section of Microsoft Entra ID. In the next section, we will cover the benefits of Configuration Manager Cloud Management Gateway.

Cloud Management Gateway

Cloud Management Gateway (**CMG**) offers a straightforward method for managing Configuration Manager clients via the internet. You set up the CMG as a cloud service in Microsoft Azure, which allows you to manage clients that are internet-roaming or located in branch offices across the WAN, without the need for additional on-site infrastructure or exposing your on-premises infrastructure to the internet.

Co-management is a system that merges your existing on-premises Configuration Manager environment with the cloud, utilizing Intune and other Microsoft 365 cloud services. You have the option to designate either Configuration Manager or Intune as the management authority for seven distinct workload groups.

As a component of Intune, co-management leverages cloud features, including Conditional Access. Some tasks remain on-premises, while others are executed in the cloud with Intune.

Co-management supports the following workloads:

- Compliance policies
- Windows Update policies
- Resource access policies
- Endpoint protection
- Device configuration
- Office Click-to-Run apps
- Client apps

Compliance policies

Compliance policies establish the regulations and configurations that a device must adhere to in order to be deemed compliant with Conditional Access policies. Additionally, compliance policies can be used to track and rectify compliance problems with devices independently of Conditional Access, starting with the Configuration Manager assessment rule.

Windows Update policies

Windows Update for Business (**WUfB**) policies let you configure WUfB policies into a ring concept so you can decide when and how you service Windows 10 and later devices.

You can set up deferral policies for Windows feature updates or quality updates for Windows 10 and later devices managed directly by WUfB. In Intune, you also have the option to configure Windows feature updates. This policy allows you to specify the Windows version to which a device should be updated, preventing it from upgrading to a newer Windows feature release.

The Windows feature build specified in the Windows 10 and later feature updates policies will remain on the device until you choose to change the policy settings. While the feature build remains static, devices will continue to download and install quality and security updates available for that feature build.

Resource access policies

Resource access policies configure **Virtual Private Network** (**VPN**), Wi-Fi, email, and certificate settings on Windows 10 and later devices.

Endpoint protection

The endpoint protection workload includes the Windows Defender suite of anti-malware protection features, such as antivirus and disk encryption.

Antivirus policies help security admins manage the settings for Microsoft Defender Antivirus, Microsoft Defender exclusions, and the Windows Security experience as a policy for Intune-managed devices.

Endpoint security disk encryption profiles focus on the settings relevant to a device's built-in encryption method, such as BitLocker, allowing IT admins to deploy and automatically encrypt end users' Windows devices. This includes BitLocker and **Personal Data Encryption** (**PDE**).

PDE is a data protection feature that encrypts select folders and their contents on PDE-deployed devices. PDE utilizes Windows Hello for Business to link data encryption keys with user credentials. This feature can minimize the number of credentials the user has to remember to gain access to content. Users will only be able to access their PDE-protected content once they've signed into Windows using Windows Hello for Business.

BitLocker drive encryption is a data protection feature that integrates with the OS and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Did you know that you can view the encryption status of all managed devices in the encryption report (**Devices** | **Monitor** | **Encryption Report**). This includes the status of encryption on the device and encryption readiness and it shows if any prerequisites are missing or if there are errors related to encryption on devices.

When integrating Microsoft Defender for Endpoint with Intune, you can use endpoint security policies for **Endpoint Detection and Response** (**EDR**) to manage EDR settings and onboard devices for Microsoft Defender for Endpoint:

- **Firewall**: You can use the endpoint security firewall policy in Intune to configure the built-in firewall on devices running Windows 10. Firewall policies are divided into two parts: the firewall policy itself and a firewall rule policy.
- **Endpoint detection and response**: When integrating Microsoft Defender for Endpoint with Intune, you can use endpoint security policies for **EDR** to manage EDR settings and onboard devices for Microsoft Defender for Endpoint.
- **App Control for Business**: This is a security practice that restricts unauthorized applications from executing in ways that put data at risk. It is a crucial aspect of endpoint security that helps businesses to only permit trusted applications to be installed and launched on their computer systems and networks.
- **Attack surface reduction**: If Defender Antivirus is in use on your Windows 11 or Windows 10 devices, use Intune endpoint security policies for attack surface reduction to manage those settings for your devices.

The attack surface reduction policy is divided into different policies:

- App and browser isolation
- Device control rules
- Device control
- Exploit protection
- Web protection for Microsoft Edge Legacy
- Application control
- Attack surface reduction rules

- **Account protection**: Account protection policies help to protect the identity and accounts of your users:
  - **Windows Local Administrator Password Solution** (**Windows LAPS**)
  - Local user group membership
  - Account protection

Windows LAPS is a Windows feature that automatically manages and backs up the password of a local administrator account on your Entra ID joined or Windows Server **Active Directory** (**AD**) joined devices.

Local user group membership policies help to add, remove, or replace members of local groups on Windows devices.

Account protection policies help protect user credentials by using technology such as Windows Hello for Business and Credential Guard.

If you switch the endpoint protection workload, the Configuration Manager policies remain on the device until they are overwritten by Intune policies or are removed by an IT admin. This ensures that the device remains protected during the transition. The same behavior applies when switching the device configuration workload, which includes policies for the Windows Information Protection feature, not included in the endpoint protection workload.

It is important to note that the Microsoft Defender Antivirus settings, which are part of the device restrictions profile type for Intune device configuration, are not included in the scope of the endpoint protection slider. To manage Microsoft Defender Antivirus for co-managed devices with the endpoint protection slider enabled, use the new antivirus policies in the Microsoft Intune admin center under **Endpoint security** | **Antivirus**. This new policy type offers new and improved options and supports all the same settings available in the device restrictions profile.

The Windows encryption feature includes BitLocker management. We will talk more about BitLocker in *Chapter 10*, *Advanced Policy Management*, and *Chapter 13*, *Identity and Security Management*.

Device configuration

The device configuration workload encompasses the settings that are managed for devices within your organization. When this workload is switched, it also transfers the resource access and endpoint protection workloads.

You can still deploy settings from Configuration Manager to co-managed devices even though Intune is the device configuration authority. This exception might be used to configure settings that your organization requires but aren't yet available in Intune. Specify this exception on a Configuration Manager configuration baseline. Enable the option to always apply this baseline even for co-managed clients when creating the baseline. You can change it later in the **General** tab of the properties of an existing baseline.

Office Click-to-Run apps

This workload manages Microsoft 365 apps on co-managed devices. Remember that when moving Microsoft 365 apps from Microsoft Intune for devices already managed by Configuration Manager, adjustments are made. These changes ensure that the Windows client is aware of deploying any Microsoft 365 Enterprise app assigned through Microsoft Intune. By shifting the workload, you do not automatically change the Microsoft 365 app update behavior on the client, but the client will not receive Office updates from Configuration Manager anymore. So, to keep your Microsoft 365 apps updated you need to shift to cloud updates from a **Content Delivery Network** (**CDN**). Updates can be managed using the settings catalog in Microsoft Intune, Windows Autopatch, or cloud update in the Microsoft 365 Apps admin center.

Office updates may take around 24 hours to show up for clients unless the devices are restarted.

Microsoft 365 Enterprise applications are managed by Intune. This condition in Intune is added by default as a requirement for new Microsoft 365 applications. When you transition this workload, co-managed clients don't meet the requirements of the application, and then they don't install Microsoft 365 deployed via Configuration Manager.

After moving the workload, Microsoft 365 apps assigned from Microsoft Intune show up in the company portal on the device.

Client apps

Use Intune to manage client apps on co-managed Windows devices. After you transition this workload, any available apps deployed from Intune are available in the company portal. Apps that you deploy from Configuration Manager are available in the software center and company portal. The company portal can show both SCCM and Intune available apps as one end user software portal.

Windows Autopilot sets up and preconfigure new devices, getting them ready for use. It is designed to simplify the life cycle of Windows devices, for both IT and end users, from initial deployment through to end of life.

As a part of Intune, you can use Autopilot to preconfigure devices and automatically enroll devices in Intune. You can also integrate Autopilot with Configuration Manager and co-management for more complex device configurations (in preview).

It is highly recommended to use Windows Autopilot in Entra ID-only environments to take advantage of the entire suite of Windows Autopilot features, such as Autopilot reset and co-management in Autopilot.

Entra ID is a service used by Intune to identify devices, users, groups, and MFA. Entra ID Premium, which is included in the Microsoft 365 license, offers additional features to help protect devices, apps, and data. These features include dynamic groups, automatic enrollment, and Conditional Access. Entra ID Premium is also required for Windows Autopilot, as automatic enrollment is a prerequisite.

Intune admin center is a centralized website for creating policies and managing your devices. It integrates with other key device management services, including groups, security, Conditional Access, and reporting. Microsoft Intune is a comprehensive solution for managing all of your devices, bringing together Configuration Manager and Intune into a single console known as the Microsoft Intune admin center.

Starting in Configuration Manager version 2002, you can upload your Configuration Manager devices to the cloud service and take action from the **Devices** blade in the admin center:

- **Client details**: This feature gives the IT admin or helpdesk a fast overview of properties and the state of devices.
- **Install applications**: This feature gives the IT admin or helpdesk the option to deploy an application to the end users' devices.
- **Device timeline**: Devices send events once a day to the admin center. Only events collected after the client receives the **Enable Endpoint analytics data collection** policy are visible in the admin center. Generate test events easily by installing an application or an update from Configuration Manager or restarting the device. Events are kept for 30 days. Use the chart to view events that are collected.
- **Resource Explorer**: From the Microsoft Endpoint Management admin center, you can view the hardware inventory for uploaded Configuration Manager devices by using Resource Explorer.
- **Run scripts**: This option allows additional IT admins or the helpdesk to run PowerShell scripts from the cloud against an individual Configuration Manager-managed device in real time. This provides all the traditional benefits of PowerShell scripts that have already been defined and approved by the Configuration Manager admin in the on-premises environment.

Enabling tenant attach has no end user impact without the IT admin creation policies and deploying them to their devices.

Microsoft Intune – from on-premises to the cloud

The unified endpoint management journey is different for each customer. Some customers will already be using some components of Microsoft Intune, so the migration is relatively easy:

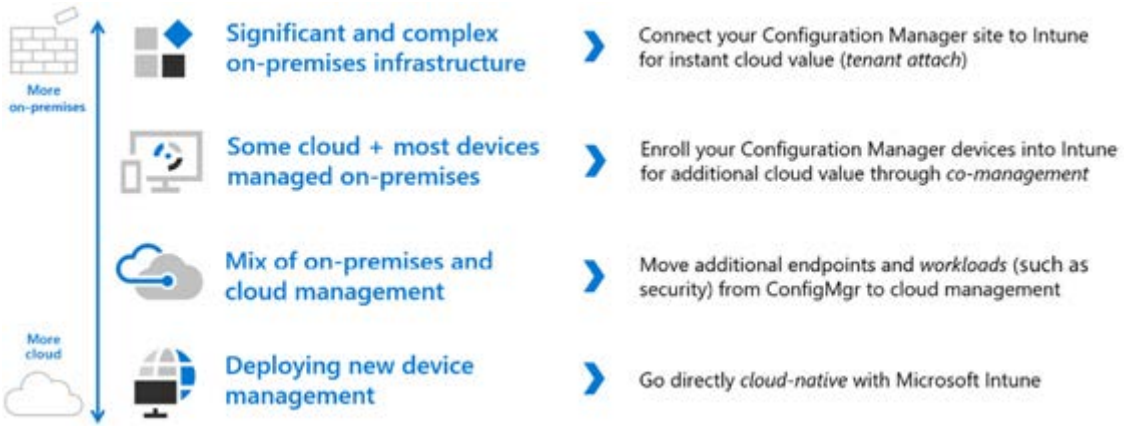


Figure 2.13: Microsoft Intune – on-premises-to-cloud flow

If you are still using complex on-premises infrastructures, the work to move to the cloud could be a bit more intense. That workload is fully dependent on the complexity of your current environment.

Exploring Windows 11 Enterprise in detail

Some Windows features are exclusive to the Enterprise edition of Windows, while certain MDM capabilities are only available for Enterprise versions. Windows 11 Enterprise offers exclusive features and services on top of those available in Windows 11 Pro. Refer to the following list of additional Enterprise features and services:

- **Intelligent security**:
  - **Credential Guard:** Protects against user credential harvesting and pass-the-hash attacks or pass-the-token attacks.
  - **Managed Microsoft Defender Application Guard (MDAG) for Microsoft Edge:** Isolates enterprise-defined untrusted sites with virtualization-based security from Windows, protecting your organization while users browse the internet.
  - **PDE:** Encrypts an individual's content using Windows Hello for Business to link the encryption keys to user credentials.
  - **Always-on VPN device tunnel**: Advanced security capabilities to restrict the type of traffic and which applications can use the VPN connection.
  - **Unified Write Filter** (**UWF**).
- **Simplified updates**:
  - 36 months of support for Enterprise Windows
  - WUfB deployment service

    - Windows Autopatch
- **Flexible management**:
    - Azure Virtual Desktop user rights
    - Microsoft **User Experience Virtualization** (**UE-V**)
    - Microsoft **Application Virtualization** (**App-V**)
    - Microsoft FSLogix profile container
    - Windows subscription activation
- **Enhanced productivity**:
    - SMB Direct
    - Persistent memory
    - Windows experience customization - `https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-experience`
- **Support for other Microsoft 365 services**:
    - Azure Virtual Desktop
    - Windows 365
    - Windows 365 Boot
    - Windows 365 Switch
    - Universal Print

This concludes this section. In the next section, we will cover Windows subscription activation.

Windows subscription activation

Subscription activation is a feature that allows you to upgrade from Windows Pro edition to Enterprise or Education editions provided that you have a subscription to Windows Enterprise E3 or E5 licenses. This feature also supports upgrading from Windows Pro Education edition to Education edition.

Subscription activation eliminates the need for manual deployment of Enterprise or Education edition images on each target device, as well as the need for on-premises key management services such as KMS or MAK-based activation, entering **Generic Volume License Keys** (**GVLKs**), and rebooting client devices.

Subscription activation for Enterprise E3 and E5 licenses is available as an online service via subscription. This allows you to deploy Windows Enterprise in your organization without keys and reboots. Devices with a current Windows Pro edition license can be seamlessly upgraded to Windows Enterprise, and product key-based Windows Enterprise software licenses can be transitioned to Windows Enterprise subscriptions. Organizations with an enterprise agreement can also benefit from this service using traditional AD-joined devices. In this scenario, the AD user signing in on their device must be synchronized with Microsoft Entra ID using Microsoft Entra Connect Sync.

Some benefits of utilizing the subscription activation feature include:

- Access to Windows 10/Windows 11 Enterprise or Education editions
- Deploying your license on up to five different devices
- The option to roll back to Windows Pro at any time
- An easy-to-manage per-user monthly payment model
- Options to move licenses between users as needed

This concludes the section on Windows subscription activation. In the next section, we will cover an overview of Windows Autopatch.

Windows Autopatch

Windows Autopatch is a new Microsoft cloud service that is included within your existing Windows E3/E5 subscriptions. With Windows Autopatch, the responsibility of managing Windows devices and patching them monthly, post Patch Tuesday, is transferred from your IT department to Microsoft. You can think of it as Windows Updates as a Service. Windows Autopatch is not the same as WUfB. New and enhanced cloud service components are combined with WUfB to deliver Windows Autopatch.

In essence, Windows Autopatch automates the planning and deployment process of Windows updates for Windows 10 and Windows 11 completely, as well as for Microsoft 365 Apps for Enterprise, Microsoft Edge, and Microsoft Teams. Not only will this simplify the management of your cloud and physical PCs, but it also mitigates the risk of having security vulnerabilities entering your environment to ultimately increase the productivity of your users.

Windows Autopatch is designed to keep at least 95% of eligible devices up to date with the latest Windows quality update within 21 days of its release. Additionally, it aims to keep at least 99% of eligible devices on a supported version of Windows, so they can continue to receive Windows feature updates. For Microsoft 365 Apps for Enterprise, Windows Autopatch aims to keep at least 90% of eligible devices on a supported version of the **Monthly Enterprise Channel** (**MEC**).

The great thing about this service is that it seamlessly integrates with Windows 365 Enterprise during the provisioning policy process, which we will explain later in the book.

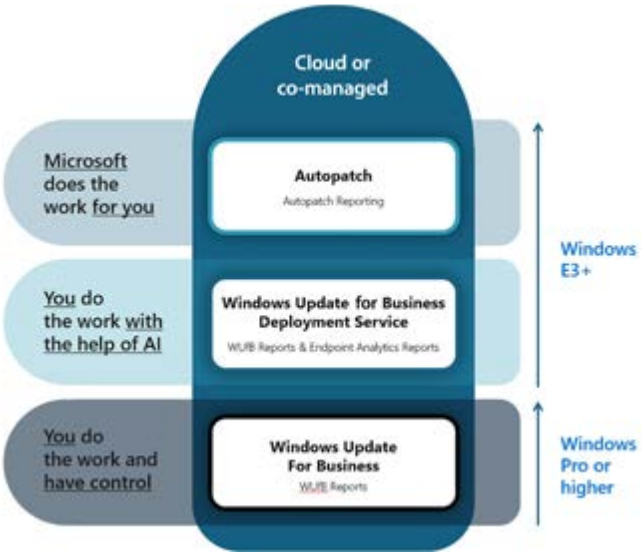


Figure 2.14: Windows Autopatch overview

Windows as a Service — update release cycle

Windows 10 will reach the end of support on October 14, 2025. The current version, 22H2, will be the last version of Windows 10, and all editions will continue to receive monthly security updates until that date.

While it is highly recommended to upgrade to Windows 11, Microsoft understands that there may be circumstances preventing you from replacing Windows 10 devices before the end of the support date. As a result, Microsoft will offer **Extended Security Updates** (**ESUs**), similar to the Windows 7 ESU program. Your organization can purchase a yearly subscription to security updates, renewable for three years. Devices enrolled in ESUs will receive monthly security updates to keep Windows 10 PCs secure.

The ESU program for Windows 10 will include critical and/or important security updates, but will not include new features, customer-requested non-security updates, or design change requests. Technical support beyond the ESU itself is also not available.

For Windows 365 customers, ESUs will be provided at no additional cost for Windows 10 devices that connect to a cloud PC running Windows 11. If you run a Windows 10 instance in Azure Virtual Desktop, ESUs will also be available at no additional charge on those virtual machines (consumption not included). More updates on the ESU program will be available as the availability date approaches, including an ESU program for individual consumers.

In the *Chapter 4*, *What is Windows 365*, we will explain how Windows 365 offers ESUs for free when using cloud PCs with Windows 11.

Windows 11 Enterprise and Education follow the Modern Lifecycle Policy, which can be found on the Microsoft website. Windows 11 will have an annual feature update cadence, a change from the semi-annual cadence of Windows 10. Windows 11 feature updates will be released in the second half of the calendar year and will come with 24 months of support for Home, Pro, Pro for Workstations, and Pro Education editions. Windows 11 will come with 36 months of support for Enterprise and Education editions, providing additional time and flexibility for the validation and at-scale deployments common on those editions. The change to an annual update cadence and slightly longer life cycle versus Windows 10 is based on user feedback and Microsoft's overall update approach.

Version	Servicing option	Availability date	Latest revision date	Latest build	End of servicing: Home, Pro, Pro Education, and Pro for Workstations	End of servicing: Enterprise, Education, IoT Enterprise, and Enterprise multi-session
23H2	General Availability Channel	2023-10-31	2023-11-14	22631.2715	2025-11-11	2026-11-10
22H2	General Availability Channel	2022-09-20	2023-11-14	22621.2715	2024-10-08	2025-10-14
21H2	General Availability Channel	2021-10-04	2023-11-14	22000.2600	End of servicing	2024-10-08

Figure 2.15: Windows 11 Enterprise release diagram

Microsoft recommends upgrading to the latest Semi-Annual Channel immediately for early adoption. This will give you the best features and user experience as soon as possible, delivered as part of Windows 10.

WUfB

WUfB enables IT professionals to use the cloud-based Windows Update service to deploy and manage Windows updates. WUfB settings, which control how and when Windows 10 or Windows 11 devices are updated, can be configured using Group Policy or MDM solutions such as Microsoft Intune.

WUfB has been available since Windows 10, version 1511, and has been improved in subsequent Windows releases, with fewer configuration options, more granular reboot options, and so on. Some of these enhancements provide IT professionals with greater control while improving the end user experience. WUfB has also evolved with the WUfB deployment service, which supports:

- Quality updates
- Feature updates
- Driver and firmware

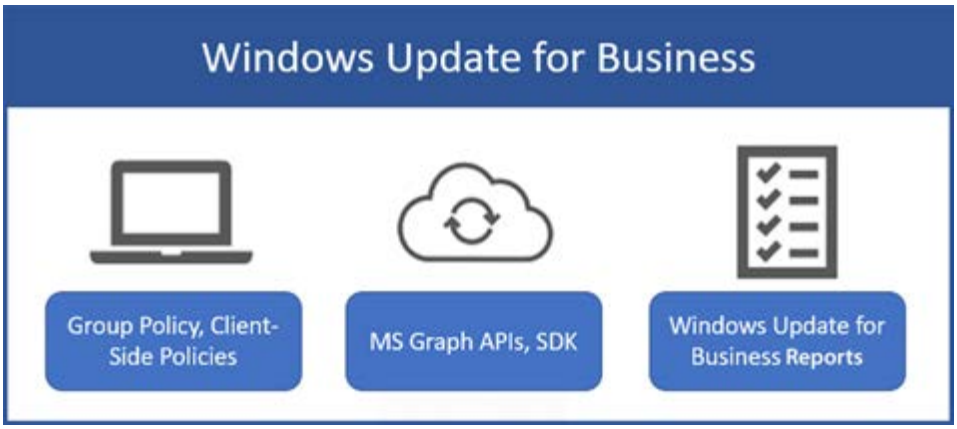


Figure 2.16: WUfB overview

Now, let's take a closer look at WUfB.

Who should use WUfB (now Autopatch)?

WUfB (now merged into Autopatch) is intended for devices running Windows Education, Professional, or Enterprise editions managed in organizations. WUfB benefits companies in the following ways:

- All organizations can leverage it to be more efficient in servicing their internet-connected devices.
- Small and medium businesses gain flexibility while continuing to use Windows Update, with more control than previously provided without using Configuration Manager, Microsoft Intune, **Windows Server Update Services** (**WSUS**), or third-party solutions.

Why do you want to leverage WUfB?

WUfB can help you to provide the end user with the best Windows update experience and lower the cost of servicing Windows while giving you much of the flexibility and control available from more complicated and time-consuming solutions:

- Reduce the cost of approving, deploying, and monitoring updates.
- Manage application compatibility within the organization's ecosystem.
- Find the right trade-offs to protect devices, while minimizing disruption to the workforce.
- Manage the infrastructure configurations necessary to support rapid update velocity, including finding the right way to address devices that are rarely connected to the enterprise.

What does WUfB allow me to configure?

When you enable the WUfB policy from Microsoft Intune with the configuration setting, WUfB will be activated. If you have previously used WSUS for servicing, your clients will connect to both Windows Update in the cloud and your WSUS server once you set WUfB settings. To change this behavior, you need to remove the old configuration settings for WSUS on the endpoints.

- WUfB provides the ability to delay the application of updates through the Windows Update Client settings, which can be configured through Group Policy, MDM, or the UX. Quality updates and feature updates are treated separately, giving you added flexibility. Additionally, you can use the **Pause** functionality if you need time to implement remediation to updates after testing them in earlier rings.
- **Feature updates**: Previously referred to as **upgrades**, feature updates contain not only security and quality revisions but also significant feature additions and changes. Feature updates are released annually in the fall.
- **Quality updates**: Quality updates are traditional OS updates, typically released on the second Tuesday of each month (though they can be released at any time). These include security, critical, and driver updates. WUfB also treats non-Windows updates (such as updates for Microsoft Office or Visual Studio) as quality updates. These non-Windows updates are known as **Microsoft updates**, and you can set devices to receive such updates (or not) along with their Windows updates.
- **Driver updates**: Updates for non-Microsoft drivers that are relevant to your devices. Driver updates are on by default, but you can use WUfB policies to turn them off if you prefer.
- **Microsoft product updates**: Updates for other Microsoft products, such as versions of Office that are installed by using Windows Installer (MSI). Versions of Office that are installed by using Click-to-Run can't be updated by using WUfB. Product updates are off by default. You can turn them on by using WUfB policies.

The policy for feature updates for Windows 10 and later works in conjunction with your update rings for Windows 10 and later policies to prevent devices from receiving a Windows feature version that is later than the value specified in the feature updates policy. For this policy to work, devices must be running Windows 10, version 1709 or later, be enrolled in Intune MDM, and be hybrid AD joined, Entra ID joined, or Entra ID registered. Windows telemetry must also be turned on with a minimum setting of Basic. If telemetry is off, devices may be upgraded to a later version of Windows than defined in the feature updates policy.

When a device receives an update ring for a Windows 10 and later policy, it updates to the version of Windows specified in the policy. If a device is already running a later version of Windows, it will remain on its current version. By freezing the version, the device's feature set remains stable for the duration of the policy.

A device will not install an update if it has a safeguard hold for that Windows version. When a device evaluates the applicability of an update, Windows creates a temporary safeguard hold if there is an unresolved known issue. Once the issue is resolved, the hold is removed, and the device can update.

Unlike using Pause with an update ring, which expires after 35 days, the Windows feature updates policy remains in effect. Devices will not install a new Windows version until you modify or remove the Windows 10 feature updates policy. If you edit the policy to specify a newer version, devices can then install the features from that Windows version.

There are over 3,000 Group Policy settings for Windows 10, and while Microsoft provides extensive guidance on different security features, exploring each one can be time consuming. You would have to determine the impact of each setting on your own and then determine the appropriate value for each setting.

WUfB for Windows has a set of policies that you can configure to provide the most secure Windows environments as it is updated, as long as the devices have internet connectivity and still maintain the best end user experience by configuring policy settings across several areas, including configuring deadlines, restart behavior, accounting for low-activity devices (active hours), delivery optimization, and power policies.

There is always a tension between the need for software update compliance and the desire to keep the workforce productive. While the security department may require a fully updated device fleet within seven days of a software update, the reality is that deploying the update has an associated cost for users, and few companies can afford to push an update on an entire workforce in the middle of a single working day unless it is a zero-day patch in an emergency. Given the competing goals of a protected and productive workforce, you may need to make choices that prioritize your business's productivity needs over maximizing update velocity.

What is the WUfB deployment service?

The WUfB deployment service is a cloud-based service within the WUfB product family. It allows you to control the approval, scheduling, monitoring, and safeguarding of content delivered from Windows Update and is designed to work in conjunction with your existing WUfB policies. The deployment service APIs, available through Microsoft Graph and associated SDKs (including PowerShell), enable you to approve and schedule specific updates for deployment. The deployment service complements existing WUfB capabilities, including device policies and the WUfB reports workbook. Microsoft Intune integrates with the deployment service to provide update management capabilities for Windows clients.

We will cover (in depth) how you can leverage WUfB deployment service in *Chapter 6*.

BYOD

Depending on the Windows **Stockkeeping Unit** (**SKU**) like Home and Pro, there are different options for BYOD. All BYOD scenarios can take advantage of Windows 365 and Azure Virtual Desktop to access either a full desktop or a single application as a remote app.

Windows devices can also be registered with Entra ID to gain access to corporate resources such as email.

Enroll the device in Intune as a personally owned device (BYOD). If an administrator has configured autoenrollment (available with Entra ID Premium subscriptions), the user only has to enter their credentials once. Otherwise, they'll have to enroll separately through MDM-only enrollment and re-enter their credentials.

Microsoft Intune management does not provide the same management capabilities on BYOD; not all Windows editions have the same MDM management setting built in:



Figure 2.17: Microsoft Intune endpoint support

Windows Enterprise has full management features, whereas both the Home and Pro editions have fewer management capabilities due to Windows limitations. Microsoft provides the option for the IT admin to leverage enrollment restrictions so that you can block personal enrollment in Microsoft Intune.

This concludes the section on BYOD. In the next section, we will cover an overview of Zero Trust.

What is zero trust?

In the past, when organizations created remote access to corporate networks, normally, access was enabled using a VPN connection either on a corporate-owned or a personally owned Windows device, only secured by an MFA token.

In today's world, organizations need a security model that can adapt to the complexities of the modern environment, accommodate a mobile workforce, and protect people, devices, applications, and data wherever they are located. This is the essence of zero trust. Instead of assuming that everything behind the corporate firewall is safe, the zero trust model operates on the assumption of a breach and verifies each request as if it originated from an uncontrolled network. No matter where the request comes from or what resource it is trying to access, the zero trust model teaches us to "never trust, always verify."

Verifying identity

The majority of security breaches today involve credential theft, and lapses in cyber hygiene amplify the potential for risk to employees and to organizations at large. That's why one of the primary components of a zero-trust system is the ability to verify a user's identity before access is granted to the corporate network.

Start by implementing MFA through the modern experience of Microsoft Authenticator and Windows Hello for Business on all Windows devices.

Verifying devices

Since unmanaged devices can be easily exploited by malicious actors, it is crucial for enterprise security to ensure that only trusted and compliant devices have access to critical applications and data. Enrolling all end user devices in device management systems such as Microsoft Intune is a fundamental aspect of our zero-trust implementation. Enabling compliance policies to check the devices for parameters such as BitLocker encryption, secure boot, and device health verification in this way is essential to managing the policies that govern access to corporate resources.

Microsoft Intune is a key piece of this new way of thinking as it makes the device trusted, with a compliance policy to validate whether the devices are compliant.

Conditional Access is a feature built into Entra ID to bring signals together, make decisions, and enforce organizational Conditional Access policies:

- **Signals:** A device or a user sign-in with a specific application or browser.
- **Decision:** The level of access you will be granted based on the policies.
- **Enforcement:** This could be as simple as giving the end user access with an MFA token or denying access:



Figure 2.18: Zero trust verifying devices diagram

At their core, Conditional Access policies are essentially if-then statements. They dictate that if a user seeks to access a corporate resource, they must first complete a specific action. For instance, if an end user wants to use the corporate Microsoft Teams application, they must do so from a compliant device in order to gain access.

IT admins and security admins have two primary goals:

- Empower users to be productive wherever and whenever.
- Protect the organization's data.

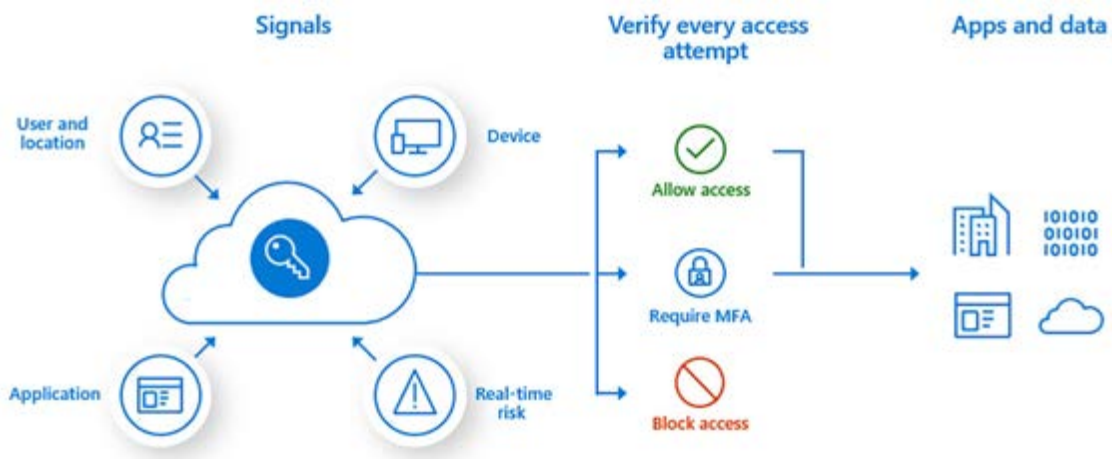


Figure 2.19: Zero trust verification process flow

By implementing Conditional Access policies, you can ensure that the appropriate access controls are applied when necessary to maintain the security of your organization while avoiding any unnecessary interference with your users. We will be going into more detail on Conditional Access and other security-related improvements in *Chapter 13*, *Identity and Security Management*.

Windows 365 for non-managed endpoints

Windows 365 is used by many enterprises to secure their environment. All the data inside the cloud PC resides in the cloud and the remoting protocol connects the client to the cloud PC over a highly secure connection.

What about BYOD – unmanaged scenarios where you have no control over the local PC? Great news – as with Windows 365, you can block access completely from the outside with RDP redirections inside Microsoft Intune – cloud PCs are very convenient to connect to a corporate managed and secure cloud PC with Windows 10 or Windows 11 from an un-managed (zero-trusted) endpoint device.

Learn more about how Intune Suite and Windows 365 bring your BYOD zero-trust security to the next level in *Chapter 11*!

Summary

In this chapter, we've learned about the fundamentals of unified endpoint management, modern management, and how this relates to Microsoft Intune. We also went through the different concepts, services, and products around Windows 11 Enterprise and security-related aspects of zero trust.

In the next chapter, we're going to talk about Windows 365 and explain this service more.

After this section, we'll continue to take a deeper dive, as we are going to talk about the different endpoint scenarios and requirements in terms of what is needed to use Microsoft Intune.

Questions

1. What license do you need for Windows Autopatch?
    a. Microsoft 365 E3
    b. Microsoft 365 E5
    c. Windows 10/11 Enterprise E3
2. What is the main principle behind zero trust?
    a. Never trust, always verify.
    b. Always trust, never verify.

Answers

1. Either A or B
2. A

Further reading

If you want to learn more about modern management after reading this chapter, please use one of the following free online resources:

- *Learn more about Windows Autopatch*: `https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/overview/windows-autopatch-faq`
- *Introduction to modern management in Microsoft 365*: `https://docs.microsoft.com/en-us/learn/modules/introduction-to-modern-management-in-microsoft-365/`
- *Modern management with Microsoft Intune* – YouTube: `https://www.youtube.com/watch?v=l03UXEnl0Fg`

Join the CloudPro Newsletter with 44000+ Subscribers

Want to know what's happening in cloud computing, DevOps, IT administration, networking, and more? Scan the QR code to subscribe to **CloudPro**, our weekly newsletter for 44,000+ tech professionals who want to stay informed and ahead of the curve.

`https://packt.link/cloudpro`

3

Requirements for Microsoft Intune

In this chapter, you will get a clear understanding of the different requirements for Microsoft Intune, from OS versions and the URL firewall allow-listing to the required licenses and privileges. Before we get started with the technical in-depth content of this book, we will cover the requirements for Microsoft Intune. Some of the requirements may not have any impact on your environment, while others will have a high impact. For example, network URL firewall requirements are not that important if you are in a zero-trust environment with all Microsoft technologies, but if for some reason you have a firewall, proxy servers, and so on in your environment, then they are highly important.

In this chapter, we'll explore the following topics:

- Endpoint scenarios
- Identity roles and privileges for Microsoft Intune
- Identity roles and privileges for a Windows 365 cloud PC
- Identity roles and privileges for Universal Print
- Licensing requirements
- Using Intune filters when assigning
- Supported OSes
- Required web browser versions
- Windows 11 hardware requirements
- How do you get Windows 11?
- Intune Administrator licensing
- Entra ID group-based licensing
- Setting the mobile device management authority
- Enabling Windows automatic enrollment
- Using Azure Virtual Desktop with Microsoft Intune
- Microsoft Intune device restrictions for Windows
- Blocking personal Windows devices
- Microsoft Intune device limit restrictions for Windows

- Customizing Intune Company Portal apps, the Company Portal website, and the Intune app
- Microsoft Intune – network URL firewall requirements
- Microsoft Store endpoint URLs
- Windows 365 endpoint URLs
- Windows Push Notification Services – required URLs
- Windows 365 and Azure Virtual Desktop – required URLs
- Universal Print – required URLs

Endpoint scenarios

Microsoft Intune supports different endpoint scenarios that we will cover in depth in this book.

The endpoint scenarios that are supported are as follows:

- Physical PC endpoints
- Cloud PC endpoints
- Mobile devices

Now that we have covered the different endpoint scenarios, we're going to explain the different roles available within Microsoft Intune.

Identity roles and privileges for Microsoft Intune

In order to configure Microsoft Intune, you first have to make sure that you have the required privileges to do so. The first user created in your Entra tenant will automatically become the global admin, as a member of the Global Admin role. The Global Admin role has the highest privileged role in Entra and can manage all facets of Microsoft Entra ID and Microsoft services utilizing Entra identities, including Microsoft Intune. To streamline user-role design, additional roles are available to assist in delegating access. For the initial setup of Intune and certain subsequent tasks, it is advisable to utilize an account with the Global Admin role.

There are also other roles that can help you in delegating access as part of your user-role design. Some of the next steps for Intune require the Global Admin role, so we recommend using this type of account for the initial setup.

In conjunction with user and device groups, you can leverage filters in Intune, which we will cover in the next section.

Using Intune filters when assigning

Intune filters is a feature of Microsoft Intune that enables administrators to filter and target specific groups of devices or users based on certain criteria. It helps admins in application or policy assignments, and filters help to remove some of the conflicts in application deployments. With filters, you as IT admin have more flexibility when it comes to assignments. This means that you can assign to a group of users or devices and leverage the filter to include or exclude devices based on attributes that are supported with filters. Filters are evaluated promptly when devices check in to the Intune service, making them significantly faster than Entra dynamic groups, which operate on a scheduled basis.

We will give you some examples of filters that can be useful when assigning different apps, policies, etc.

To start creating filters, you need to follow these steps:

1. In the Intune portal, go to **Tenant admin** | **Filters**.
2. Click **Create**.
3. In the first example, we will create a filter for AVD Multi session.
    - Enter a **Filter name**: `AVD Multi session`
    - Select a **Platform**: `Windows 10 and Later`

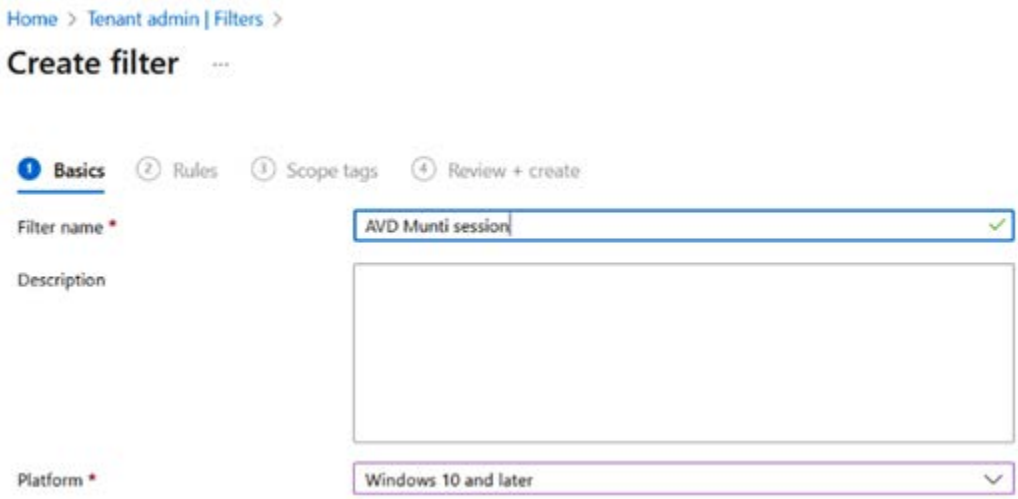


Figure 3.1: AVD Multi session filter

4. In the **Rules** section, fill in the following details:
    - **Choose a Property** | **rule builder**: `operatingSystemSKU (Operating System SKU)`
    - **Operator**: `Equals`

- **Value:** `ServerRdsh (Windows 10/11 Enterprise multi session (175))`

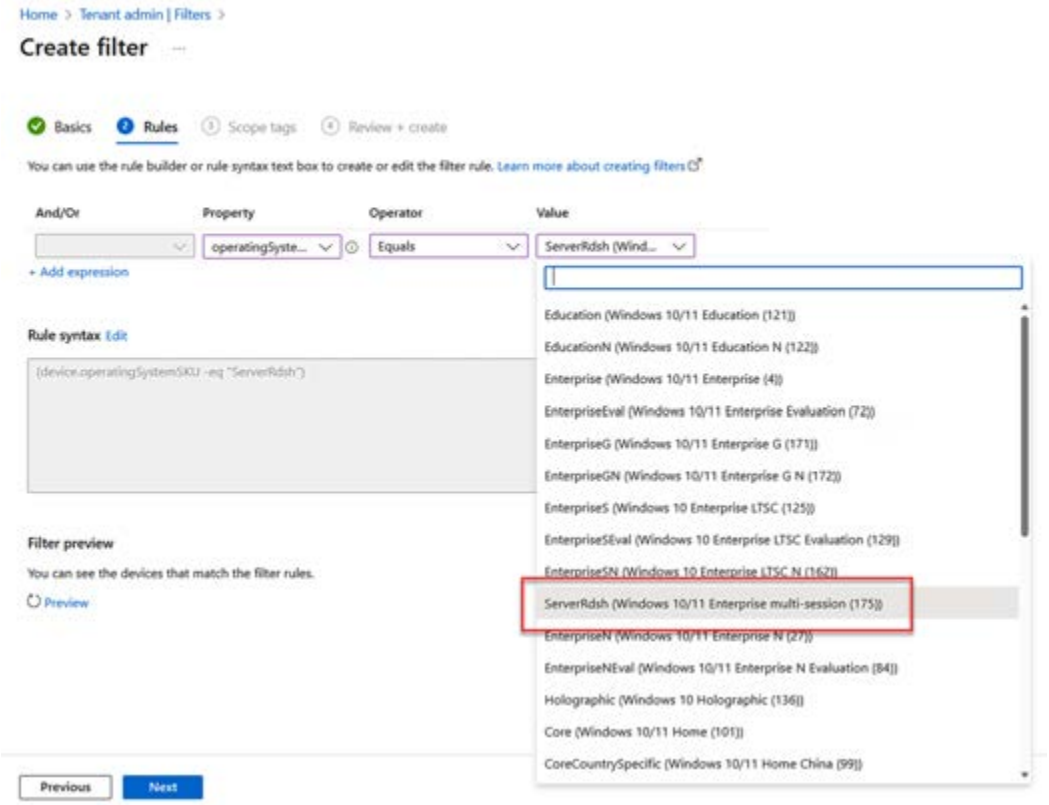


Figure 3.2: Value ServerRdsh

This gives you a rule syntax (`device.operatingSystemSKU -eq "ServerRdsh"`).

Here are some other examples of rule syntax:

- Windows 11 filter:
  - `(device.osVersion -startsWith "10.0.22")`
- Manufacturer filters:
  - `(device.manufacturer -eq "Microsoft")`
  - `(device.manufacturer -eq "LENOVO")`
- Model filters:
  - `(device.model -eq " Surface Pro 9")`
  - `(device.model -in ["Surface Book 3", "Surface Book 2"])`
  - `(device.model -startsWith "Surface Book")`

- Enrollment profile name:
    - `(device.enrollmentProfileName -eq "Autopilot HL2")`
    - `(device.enrollmentProfileName -eq "Windows Autopilot Local admin")`
    - `(device.enrollmentProfileName -startsWith "Windows AutoPilot KIOSK")`
- deviceTrustType (Microsoft Entra join type):
    - `(device.deviceTrustType -eq "Azure AD  joined")`
    - `(device.deviceTrustType -ne "Azure AD  registered")`
    - `(device.deviceTrustType -in ["Hybrid Azure AD  joined","Azure AD  joined"])`

When using some of the filters that we just have described, like an OS version such as `device.osVersion`, you can target a policy or apps more dynamically than with Entra groups alone. You can deploy a specific Win32 app that is hardware vendor-specific, which means it only applies to that hardware type. An example of that could be Lenovo or HP update tools that you only want to deploy to those models. Another example is creating a compliance policy where you want to exclude HoloLens, as they do not support the same policies as Windows Desktop does.

Possibilities with filters:

- Assign policies and apps to a specific group of devices or users based on criteria in your filters.
- Dynamically target managed devices based on a device.
- Include or exclude devices or apps in a specific group based on the criteria you enter.
- Create a query of device properties based on different properties, like **TrustType**, an enrollment profile, model, vendor, etc.

In addition, using filters can help you reduce latency in an assignments workload and improve deployment performance, especially in large Intune environments, as filters are evaluated with device check-in into Microsoft Intune, unlike Entra dynamic groups that run on a schedule.

This concludes the section on Intune filters; next up, we have a list of built-in Entra roles that are supported within Microsoft Intune. These roles can be set using the Entra admin portal.

Compliance Administrator

Users with this role have permission to manage compliance-related features in the Microsoft 365 compliance center, Entra ID, the Microsoft 365 admin center, and Microsoft compliance center.

Users with this role can also view all Intune audit data.

Compliance Data Administrator

Users with this role have permission to track data in the Microsoft 365 compliance center, the Microsoft 365 admin center, and Entra ID.

Users with this role can view all Intune audit data.

Intune Administrator

Users with this role have global permissions within Microsoft Intune.

The Intune Administrator role contains the ability to manage users and devices to associate policies, as well as to create and manage all security groups in Entra.



NOTE

The Intune Administrator role does not have admin rights over Office groups, only security groups.

Message Center Reader

Users in this role can monitor notifications and advisory health updates in the Message center for their organization within Microsoft Intune. These messages can be reviewed in **Tenant administration** | **Tenant status** | **Service health and message center**.



NOTE

This is important for scoped Intune administrator users.

Security Administrator

Users with this role have permission to manage security-related features in the Microsoft 365 security center, Entra authentication, Entra Identity Protection, Azure Information Protection, and the Microsoft 365 compliance center.

Users in this role can view user, device, enrollment, configuration, and application information. However, they cannot make changes to Intune.

Security Operator

Users with this role can manage alerts and have global read-only access to security-related features, including all information in the Microsoft 365 security center, Identity Protection, Entra, Privileged Identity Management, and the Microsoft 365 compliance center.

Users in this role can view user, device, enrollment, configuration, and application information. However, they cannot make changes to Intune.

Security Reader

Users with this role have global read-only access to security-related features, including all information in the Microsoft 365 security center, Entra, Privileged Identity Management, Identity Protection, and Microsoft 365 compliance center, as well as the ability to read Entra sign-in reports and audit logs.

Users in this role can view user, device, enrollment, configuration, and application information. However, they cannot make changes to Intune.

Identity roles and privileges for a Windows 365 Cloud PC

Now, we will see the various identity roles and privileges for a Windows 365 Cloud PC. A Windows 365 Cloud PC is supported by two different identity types, hybrid identity or cloud-only identity. External identities are not supported by Cloud PCs.

Devices can either be Entra hybrid joined or Entra joined.

Azure Subscription Owner

Users with this role have global access to all resources in the Azure subscription. These rights are needed for the initial setup of Windows 365.

This role grants users full access to manage all resources, including the ability to assign roles in Entra RBAC.

Domain Administrator

Users with this role will be able to create computer accounts in your on-premises domain. This is needed to create the computer accounts for cloud PCs in your domain. You can also delegate access via delegation of control directly to the right organizational unit in your domain.

Identity roles and privileges for Universal Print

Universal Print introduced two roles, Printer Administrator and Technician, to Entra. The Printer administrator is needed to do the initial configuration.

We will talk more about Universal Print later on in the book:

- Printer Administrator:
    - Users in this role have full access to manage all aspects of printers in Universal Print.
- Printer Technician:
    - Users in this role can register and un-register printers and set the printer status.

Licensing requirements

To use Microsoft Intune, you have to be assigned an Intune license. There are also options to obtain a trial license for 30 days to kick the tires and validate the service.

Microsoft Intune as a service doesn't require an Azure subscription. With Windows 365 + Entra ID join, an Azure subscription is not necessary. However, when you use the service with Hybrid Entra ID join, you'll need to set up an Azure virtual network, and therefore, you'll need an Azure subscription.

Here are the types of licenses that provide access to Microsoft Intune:

- Intune-only license
- Microsoft 365 E3
- Microsoft E5
- **Enterprise Mobility + Security** (**EMS**) E5

It's likely that your company already owns one of these licenses and, therefore, already has access to Microsoft Intune.

Creating a trial account is relatively easy; you just go to `https://admin.microsoft.com` and click on **Billing**, followed by **Purchase services**. Search for one of the licenses listed previously and purchase the trial (for free). There's no credit card or any other payment details needed for this process:



Figure 3.3: Microsoft 365 license purchase

Supported OSes

In this section, we'll look at the OSes and web browser versions that support Microsoft Intune. Let's first look at the OSes:

- Microsoft:
    - Windows 11 (Enterprise single- and multi-session versions)
    - Windows 10 (Enterprise single- and multi-session versions)
    - Windows 10 Pro Education
    - Windows 10 Enterprise 2019/2021 LTSC
    - Windows 10 IoT Enterprise (x86, x64)
    - Windows 10 Teams – Surface Hub
    - Windows Holographic for Business
- Supported mobile OSes:
    - Apple:
        - Apple iOS 15.0 and later

    - Apple iPadOS 15.0 and later
    - macOS X 11.0 and later
- Google:
    - Android 8.0 and later (including Samsung Knox Standard 3.0 and higher)
    - Android Enterprise
    - Android open source project device

Next, we will see what versions of web browsers support Microsoft Intune.

Required web browser versions

Depending on your specific IT admin tasks, you might use one of the following admin portals:

- Microsoft Intune admin portal
- Microsoft 365 admin portal
- Entra admin center

The following browsers are supported for these portals:

- Microsoft Edge (latest version)
- Safari (latest version – Mac only)
- Chrome (latest version)
- Firefox (latest version)

Now that we know about the OS and browser requirements, let's take a look at the hardware requirements for Windows 11.

Windows 11 hardware requirements

Windows 11 is now on its third release after **GA** (**General Availability**).

However, there are some fundamental changes to the requirements of the hardware for Windows 11 compared to Windows 10 that we would like to explain:

- **Processor**: 1 **Gigahertz** (**GHz**) or faster with two or more cores on a compatible 64-bit processor (`https://aka.ms/CPUlist`) or **System on a Chip** (**SoC**).
- **RAM**: 4 **Gigabytes** (**GB**) or greater.
- **Storage**: 64 GB* or greater available storage is required to install Windows 11 (additional storage space might be required to download updates and enable specific features).
- **Graphics card**: Compatible with DirectX 12 or later, with a WDDM 2.0 driver.
- **System firmware**: UEFI and Secure Boot-capable.
- **TPM**: **Trusted Platform Module 2.0** (`https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview`).
- **Display**: High-definition (720p) display, 9" or greater monitor, and 8 bits per color channel.
- **Internet connection**: Internet connectivity is necessary to perform updates.

**There might be additional requirements over time for updates and to enable specific features within the OS.*

The requirements are important to follow as you might run into complications once you start upgrading to Windows 11:

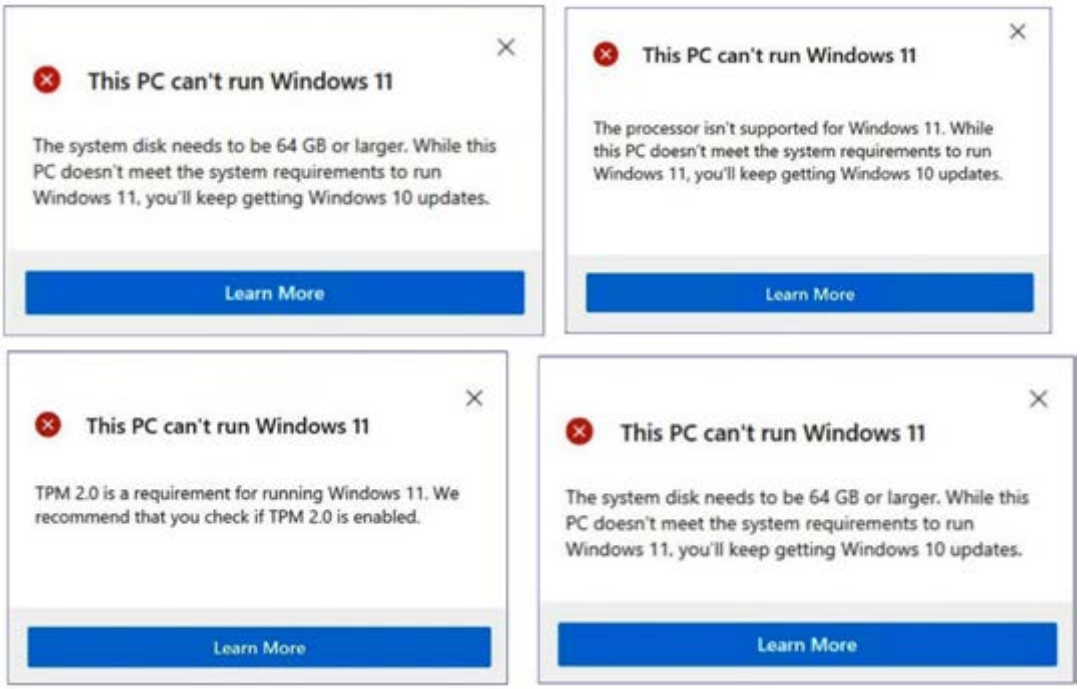


Figure 3.4: Compatibility errors

You can see screenshots of errors in the Windows 11 installation process in the preceding figure. It detects the hardware requirements before you can start the in-place upgrade process.

There are also some other differences between Windows 10 and 11 that you must know about before upgrading. You can find them in the following list:

- Start is significantly changed in Windows 11, including the following key deprecations and removals:
    - Live tiles
    - Dynamic previews
    - Named groups and folders of apps
- Pinned apps and sites will not migrate when upgrading from Windows 10.
- New modern icons for Windows.
- The Windows Store app has been updated and allows the installation of Win32 applications.
- A new feature with the flexibility of multiple windows and the ability to snap apps side by side.
- Live tiles are no longer available. For glanceable, dynamic content, please check out the new widgets feature.

- Tablet mode is removed, and new functionality and capabilities are included for keyboard attach and detach postures.
- Taskbar functionality has changed, including the following:
    - **People** is no longer present on the taskbar.
    - Some icons may no longer appear in the **system tray** (**systray**), including previous customizations for upgraded devices.
    - Only alignment to the bottom of the screen is allowed.
    - Apps can no longer customize areas of the taskbar.
    - **Timeline** is removed. Some similar functionality is available in Microsoft Edge.
    - **Internet Explorer** is removed. Edge is the recommended replacement and includes IE mode, which may be useful in certain scenarios.
    - **Math Input Panel** is removed.
    - **Snipping Tool** continues to be available, but the old design and functionality in the Windows 10 version have been replaced with those of the app, previously known as Snip & Sketch.
    - Center alignment on the desktop.

You can see the new desktop experience and the layout of Windows 11 in the following screenshot:



Figure 3.5: Windows 11 UI

How do you get Windows 11?

Windows 11 21H1 has been generally available since 4th October 2021 and is end of service for Pro versions – Enterprise/Education versions will end their service on 8th October 2024. Since that release, two additional versions were released, namely Windows 11 22H2 (September 20, 2022) and Windows 11 23H2 (October 31, 2023).

Learn more about Windows 11 release information here: `https://learn.microsoft.com/en-us/windows/release-health/windows11-release-information`

This concludes the section on Windows 11; in the next section, we will cover how to configure Intune Administrator Licensing.

Intune Administrator Licensing

All Intune administrators need a Microsoft Intune license by default. You can change this in the Microsoft Intune admin center (`https://intune.microsoft.com`) at a later point, allowing you to give administrators access to Microsoft Intune without requiring an Intune license.

To get an administrator license, you need to follow these steps:

1. Go to **Tenant admin** | **Roles** | **Administrator Licensing**.
2. Click **Allow access to unlicensed admins**:

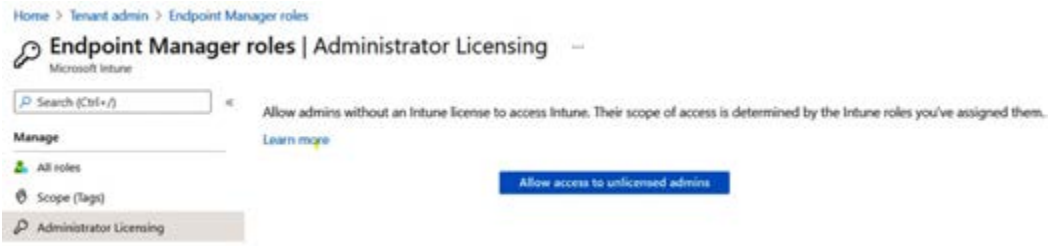


Figure 3.6: Microsoft Intune admin center – Administrator Licensing



NOTE

You cannot revert this setting once it is set.

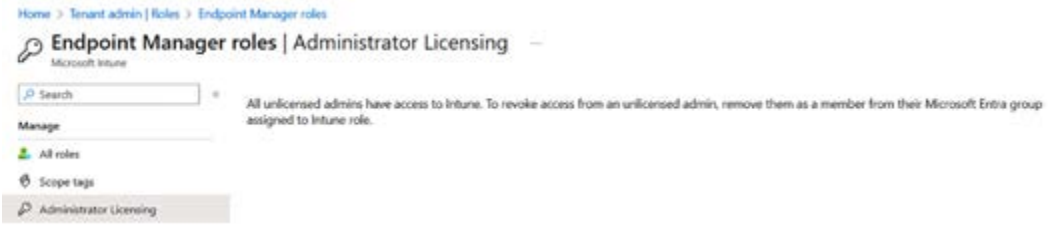


Figure 3.7: Microsoft Intune admin center – Administrator Licensing after the change

3. In the Microsoft 365 admin center, go to `https://admin.microsoft.com`. If you are a global admin, you can assign your Intune license:

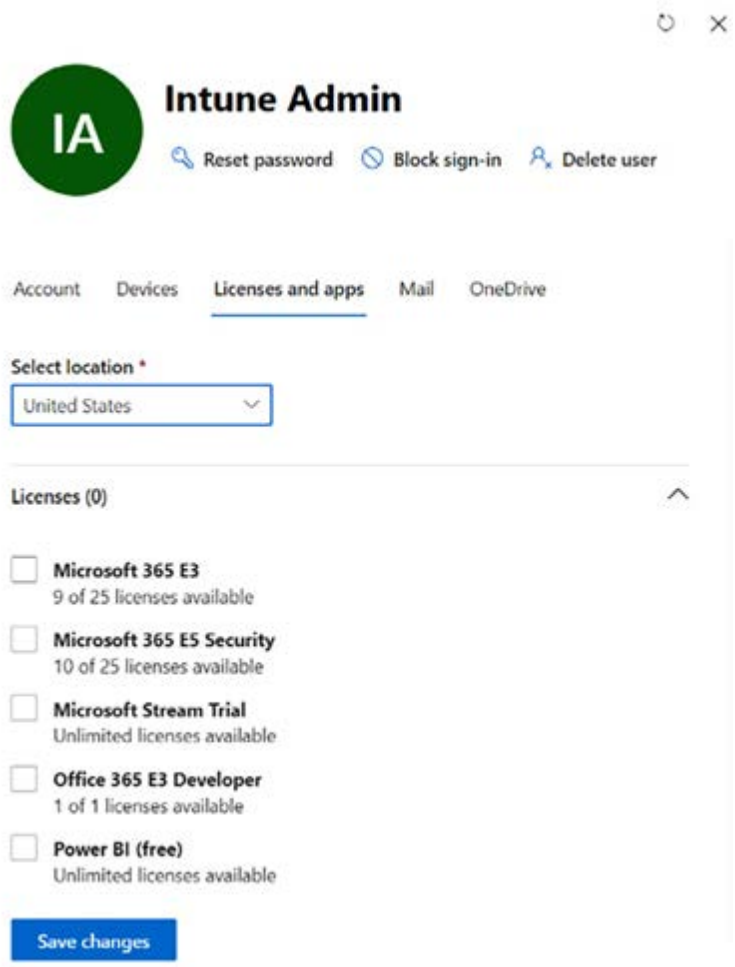


Figure 3.8: Microsoft 365 admin center – license assignments

The Microsoft Intune license is a part of Microsoft 365 E3/E5, Microsoft 365 F1/F3 for Firstline Workers, EMS E3, as well as standalone Microsoft Intune.

There are many other licenses that give you access to Microsoft Intune. Always consult your license partner to find out the correct license for your scenario.

A user in your tenant also requires a license to enrol their device into Intune.

One suggested approach for allocating Intune licenses to your users is to utilize Entra group-based licensing.

Entra group-based licensing

Microsoft paid cloud services, such as Microsoft 365, EMS, Windows 10, Office 365, Dynamics 365, and other similar products, require licenses. These licenses are assigned to each user who needs access to these services. Administrators use one of the management portals (`https://admin.microsoft.com` or `https://entra.microsoft.com`) and PowerShell cmdlets to manage licenses. Entra is the underlying infrastructure that supports identity management for all Microsoft cloud services. Entra stores information about license assignment states for users.

Entra includes group-based licensing, which means one or more product licenses can be assigned to a group. Entra ensures that the licenses are assigned to all members of the group. This includes non-members who then become a member of the group. When they leave the group, those licenses are removed. This licensing management eliminates the need for automating license management via PowerShell to reflect changes in an organization and departmental structure on a per-user basis.

For any group assigned a license, you must also have a license for each unique member. While you do not have to assign each member of the group a license, you must have at least enough licenses to include all the members. For example, if you have 10,000 unique members who are part of licensed groups in your tenant, you must have at least 10,000 licenses to meet the licensing assignment.

Licenses can be assigned to any security group in Entra. Security groups can be synced from on-premises using Entra Connect. You can also create security groups directly in Entra (also called cloud-only groups), or automatically via the Entra dynamic group feature. Office 365 groups cannot be used for group-based licensing.

When a product license is assigned to a group, one or more service plans in the product can be disabled by the administrator. Typically, this assignment is done when the organization is not yet ready to start using a service included in a product. For example, the administrator might assign Microsoft 365 to a department but temporarily disable the Yammer service.

Entra automatically manages license modifications that result from group membership changes. Typically, license modifications are effective within minutes of a membership change.

A user can be a member of multiple groups with license policies specified. A user can also have some licenses that were directly assigned, outside of any groups. The resulting user state is a combination of all assigned product and service licenses. The license will be consumed only once if a user is assigned the same license from multiple sources.

In some cases, licenses cannot be assigned to a user. For example, there might not be enough licenses available in the tenant or conflicting services might have been assigned at the same time. Administrators have access to information about users for whom Entra could not fully process group licenses. They can then take corrective action based on that information.

Setting the mobile device management authority

As an IT admin, you *must set* a **Mobile Device Management** (**MDM**) authority before users can enrol devices for management.

Automatic enrollment lets users enrol their Windows 10 and later devices in Intune. Users need to add their work account to their personally owned devices or join corporate-owned devices to Entra to enrol. In the background, the device registers and joins Entra. Once registered, the device is managed with Microsoft Intune, provided that the user is licensed for Microsoft Intune.

All applications and policies assigned to their username or device will start being deployed.

Enabling Windows automatic enrollment

Automatic MDM enrolment means when a Windows device joins Entra, the device will automatically be enrolled into Intune with the MDM enrollment flow.

To configure automatic Windows enrollment, follow these steps:

1. In the Microsoft Intune admin center, go to **Devices** | **Windows** | **Windows enrollment** followed by **Automatic Enrollment**:

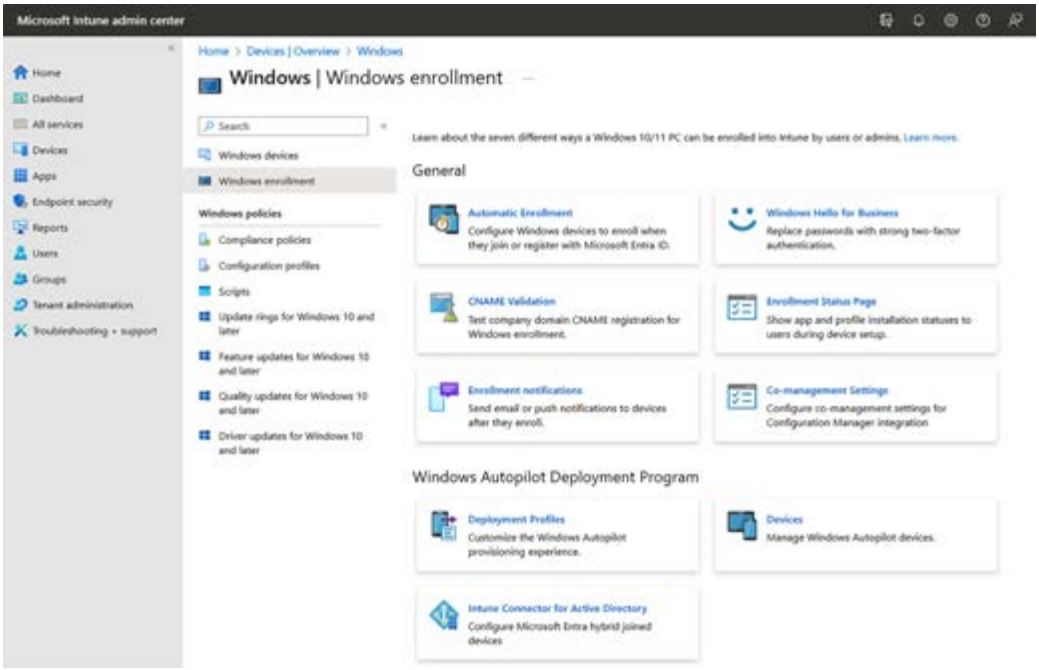


Figure 3.9: Microsoft Intune admin center – Windows automatic MDM enrollment

User enrollment can also be scoped to a group of users, if all your users have an Intune license assigned. The best option is to leverage Intune enrollment restriction to configure which Windows devices a user can enrol.

2. Make sure to select **All** for **MDM user scope:**

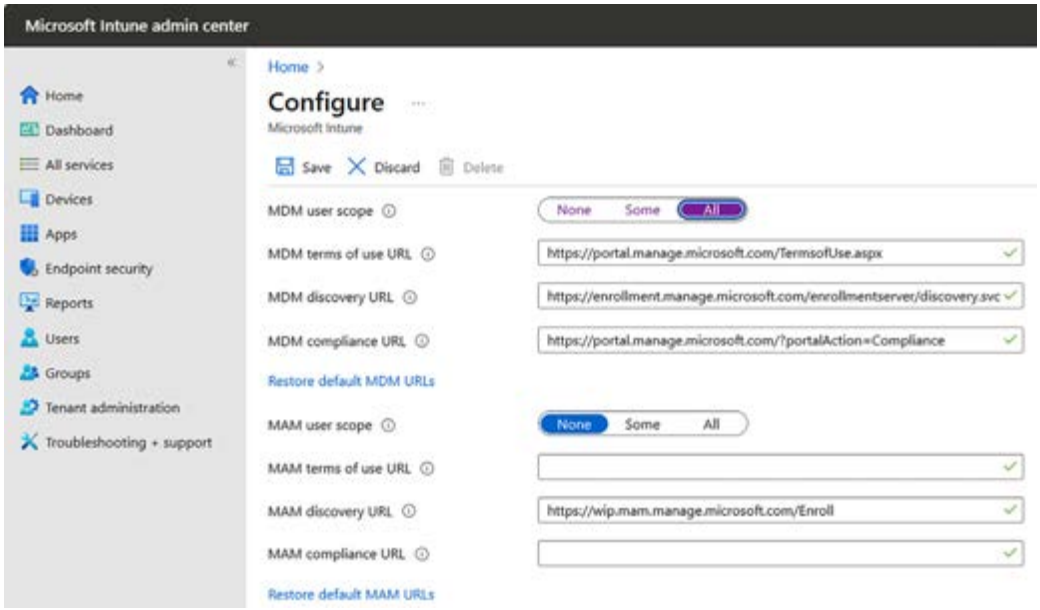


Figure 3.10: Microsoft Intune admin center – MDM user scope

Here's what all the options for **MDM user scope** mean:

- **None:** MDM automatic enrollment is disabled.
- **Some:** Select the groups that can automatically enroll their Windows devices.
- **All:** All users can automatically enroll their Windows devices.



NOTE

Automatic MDM enrollment requires an Entra Premium subscription.

For Windows **Bring Your Own Device** (**BYOD**) devices (personal enrollment), the **Mobile Application Management** (**MAM**) **user scope** takes precedence if both the MAM user scope and the MDM user scope (automatic MDM enrollment) are enabled for all users (or the same groups of users).

The Windows Information Protection without enrollment scenario in Microsoft Intune is no longer supported, and you are not able to create a new policy for that scenario.

If you encounter a warning like this:

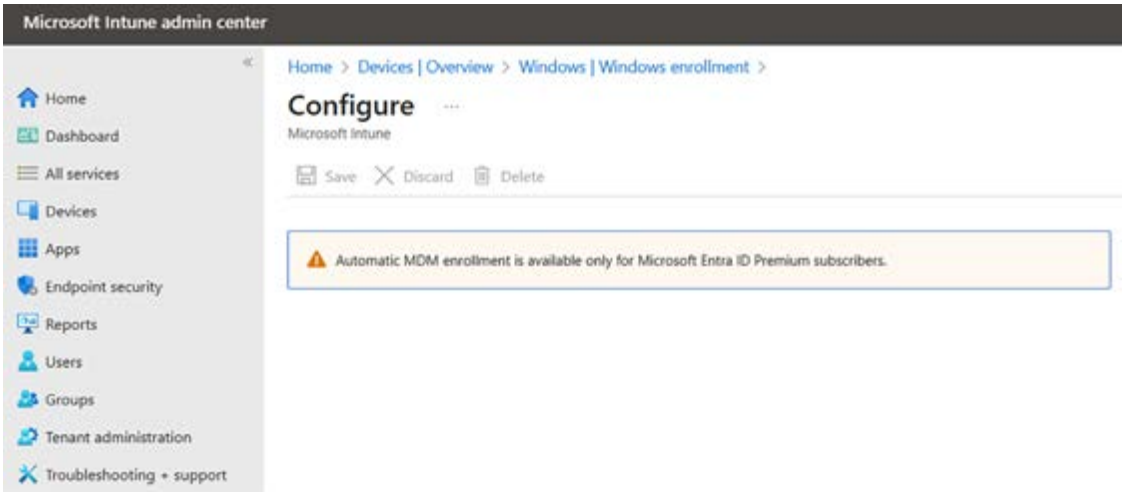


Figure 3.11: Microsoft Intune admin center – Automatic MDM enrollment

It means that you do not have an active Entra ID Premium subscribe in your tenant.

This concludes the section on automatic MDM enrolment; in the next section, we will cover using Azure Virtual Desktop with Microsoft Intune.

Using Azure Virtual Desktop with Microsoft Intune

The following steps are not needed within Windows 365, as the enrolment into Intune happens automatically. Also, make sure that you have followed the previous step (setting **MDM user scope** to **All** and **MAM user scope** to **None**) before continuing.

Prerequisites:

- Running Windows 10 Enterprise, version 1809 or later, or running Windows 11.
- Set up personal remote desktops in Azure.
- Microsoft Entra hybrid joined and enrolled in Intune in one of the following methods:
    - Configure Active Directory group policy to automatically enrol devices that are Microsoft Entra hybrid joined.
    - Configuration Manager co-management.
    - User self-enrollment via Microsoft Entra join.
    - Microsoft Entra joined and enrolled in Intune by enabling **Enroll the VM with Intune** in the Azure portal.



NOTE

Make sure that the **RemoteDesktopServices/AllowUsersToConnectRemotely** policy isn't disabled on your AVD devices.

Keep in mind that the following Windows 10 desktop device remote actions aren't supported/recommended for Azure Virtual Desktop virtual machines:

- Autopilot reset
- BitLocker key rotation
- Fresh start
- Remote lock
- Reset password
- Wipe and Retire

Deleting VMs from Azure leaves orphaned device records in Intune. They'll be automatically cleaned up if the built-in cleanup rules are configured for the tenant.

Let's get started configuring the GPO that configures automatic MDM enrolment for Hybrid Entra joined devices with a device token:

1. Log on to your session host.
2. Open **Local Computer Policy** and click **Administrative Templates** | **Windows Components** | **MDM**:

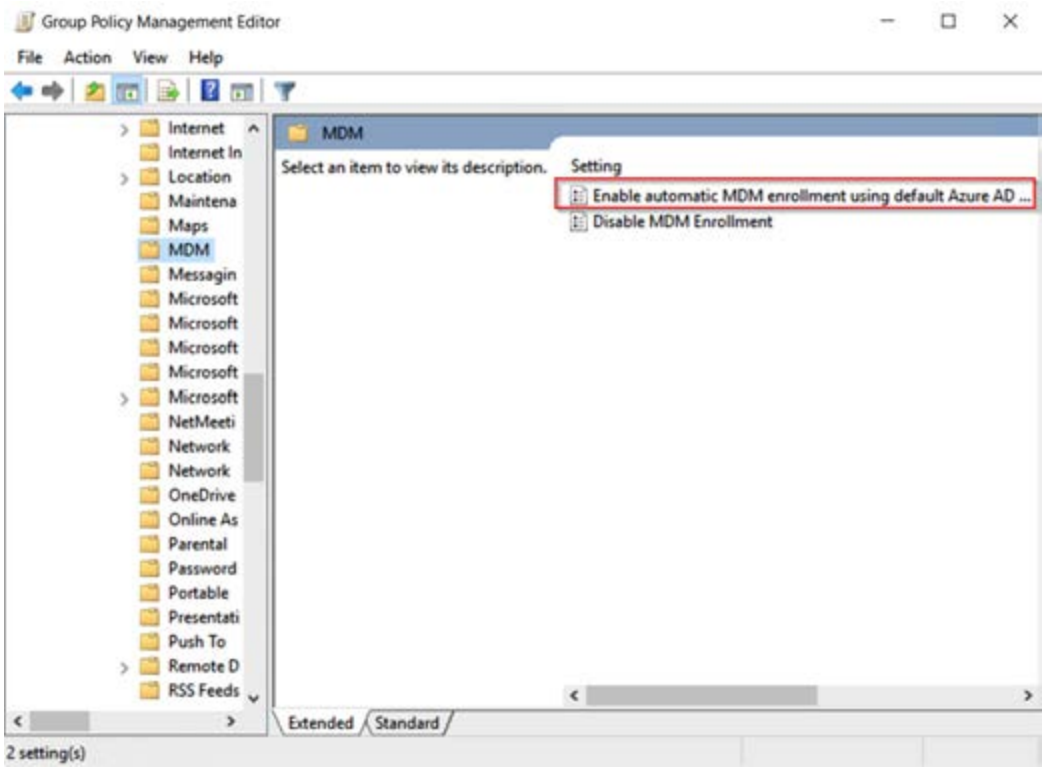


Figure 3.12: Local group policy – MDM

3. Set the policy to **Enabled**.

4. Set the credential type to **Device Credential:**

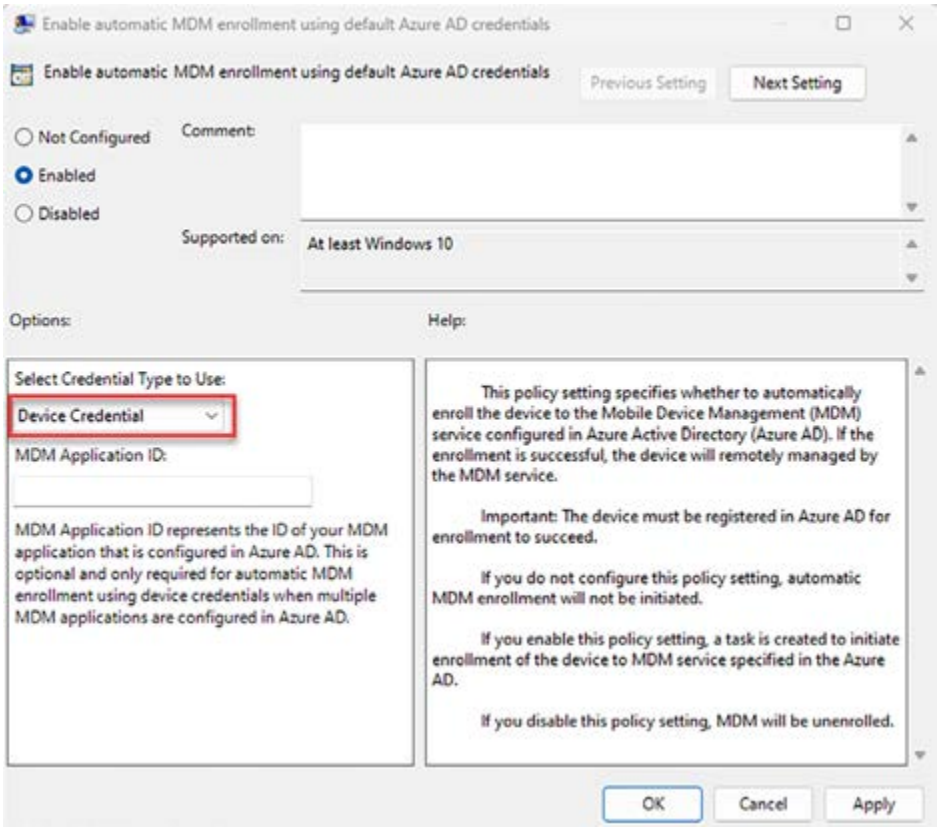


Figure 3.13: Local group policy – MDM

5. Confirm the MDM enrollment of your session hosts into Entra, which should look like the following examples:

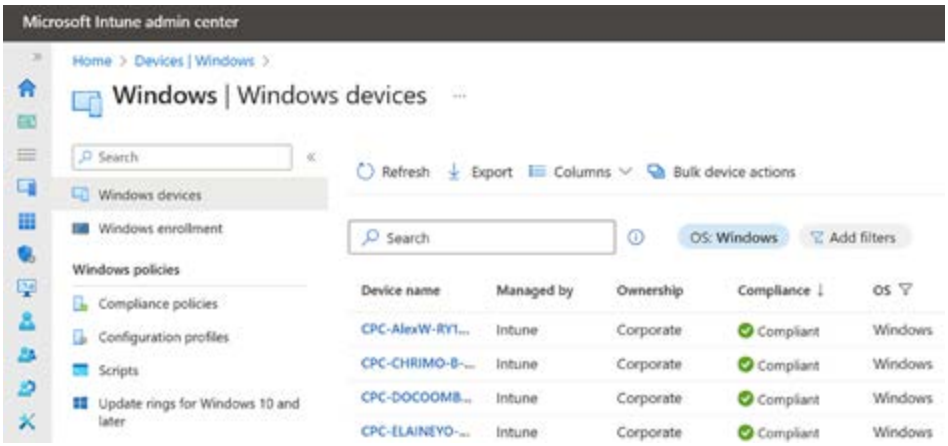


Figure 3.14: Admin center – all Windows devices

We have just shown you the different options for enrolling Windows devices into Microsoft Intune; we will now show you how you can limit Windows enrollment with Microsoft Intune enrollment restrictions.

Microsoft Intune device restrictions for Windows

In this section, we will see how to create enrollment restrictions for Windows devices:

1. Sign in to the Microsoft Intune admin center (`intune.microsoft.com`).
2. Select **Devices** | **Enrollment device platform restrictions**:

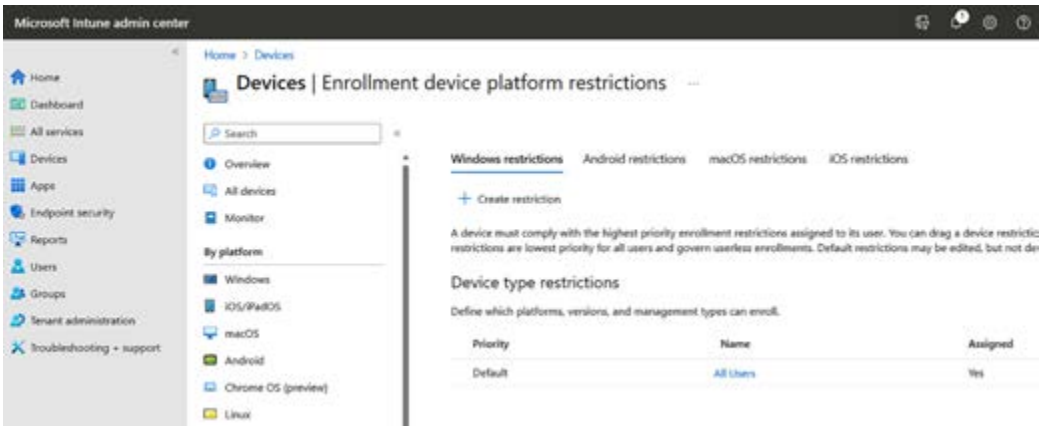


Figure 3.15: Admin center – Enrollment device platform restrictions

3. Create a restriction. Enter `Device type restriction – HR` as the name:

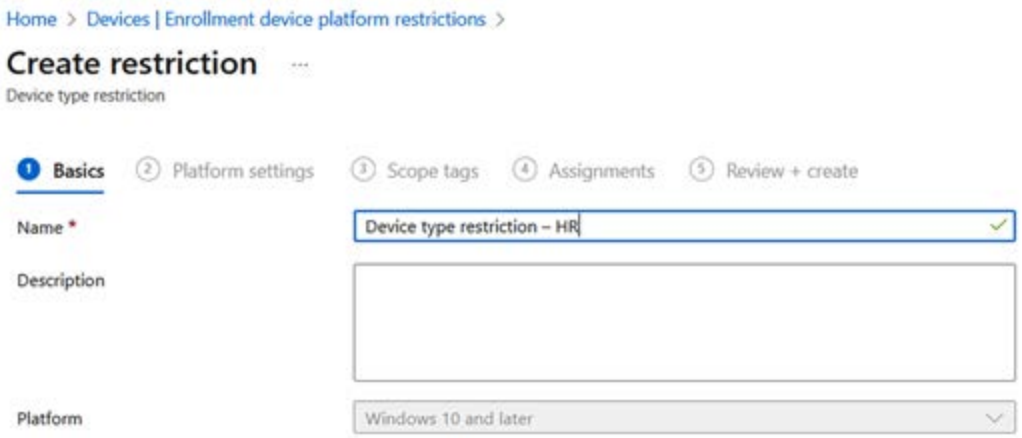


Figure 3.16: Admin center – enrollment restrictions

4. Select the block and allow both for MDM and personally owned devices to allow or block Windows enrollment.

If you are allowing Windows (MDM) platform enrollment, you can block personal devices; see the following section to understand what *blocking personal Windows devices* means.

Allow min/max range for the OS version only blocks devices on enrollment and has no effect on devices already enrolled into Microsoft Intune; enrollment restriction is only validated on enrollment.



NOTE

Windows supports the `major.minor.build.revision` format for Windows.

Windows does not provide the rev number during enrollment, so, for instance, if you enter `10.0.22631.2000` and the device is `10.0.22631.2428`, it will be blocked during enrollment.

You can always open a Command Prompt and type `ver`. The `ver` command returns the number in the correct format.

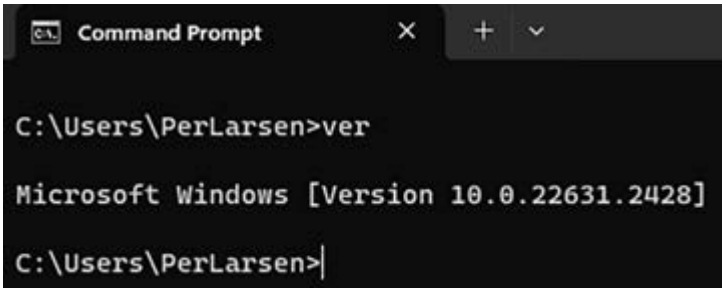


Figure 3.17: Command Prompt – ver



Figure 3.18: Admin center – enrollment restrictions – Platform settings

5. For the **Assignments** step, select **HR Department.**

   When you are creating a custom enrollment restriction, you can scope it to apply to specific user groups in your organization, departments, countries, and so on.

Change the assignment settings to filter, based on any restrictions you want to provide to avoid groups from enrolling into MDM Intune:

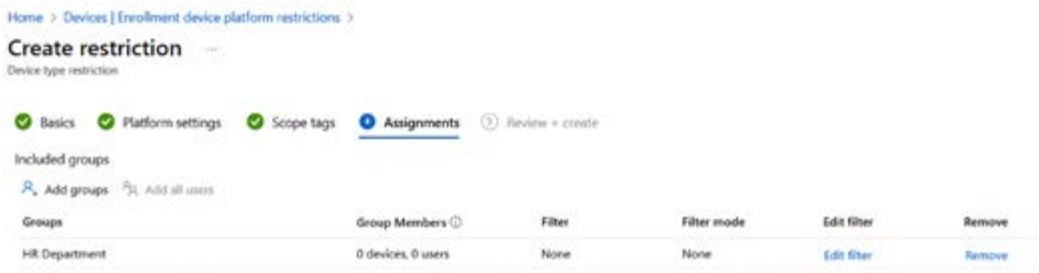


Figure 3.19: Admin center – enrollment restrictions – Assignments

6. In the following screenshot, you can see an overview of the default device type restrictions:



Figure 3.20: Admin center – Windows restrictions

In the next section, let's see how to block personal devices.

Blocking personal Windows devices

If you block personally owned Windows devices from enrollment, when a new device is being enrolled into Microsoft Intune, the Intune backend enrolment service will verify that the devices go through one of the corporate enrollment workflows. If the devices do not go through the corporate enrolment workflow, the Windows MDM enrolment will be blocked.



NOTE

Blocking Windows MDM enrollment in the default enrollment restriction will block some scenarios with corporate devices.

Since a co-managed and Autopilot self-deploying mode device enrolls in the Microsoft Intune service based on its Microsoft Entra device token, and not a user token, only the default Intune enrollment restriction will apply to it.

This is a list of the enrolment methods that are considered Windows corporate enrollments:

- The enrolling user uses a device enrollment manager account.
- The device enrolls through Windows Autopilot.
- The device is registered with Windows Autopilot but isn't an MDM enrollment-only option from Windows settings.
- The device enrolls through a bulk provisioning package.
- The device enrolls through a **Group Policy Object** (**GPO**), either in a user or device context, or automatic enrollment from Configuration Manager for co-management.

The following enrollments are marked as corporate by Intune. However, since they don't offer the Intune administrator per-device control, they'll be blocked:

- Automatic MDM enrollment with an Entra join during OOBE Windows setup*
- Automatic MDM enrollment with an Entra join from a Windows settings *app**

The following personal enrollment methods will also be blocked:

- Automatic MDM enrollment with **Add Work Account** from a Windows settings *app**
- The MDM enrollment-only option from Windows settings



NOTE

These won't be blocked if registered with Autopilot, as the device will be registered as a corporate device.

This concludes the section about enrolment restrictions; in the next section, we will cover device limits for Intune enrolment.

Microsoft Intune device limit restrictions for Windows

In this section, we will learn how to limit the restrictions for a device. Let's get started.

To configure the enrollment restriction for Windows, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Devices** | **Windows** | **Windows Enrollment** | **Device limit restriction** and **Create restriction**:
    - **Name**: Enter `Device limit restriction – HR`

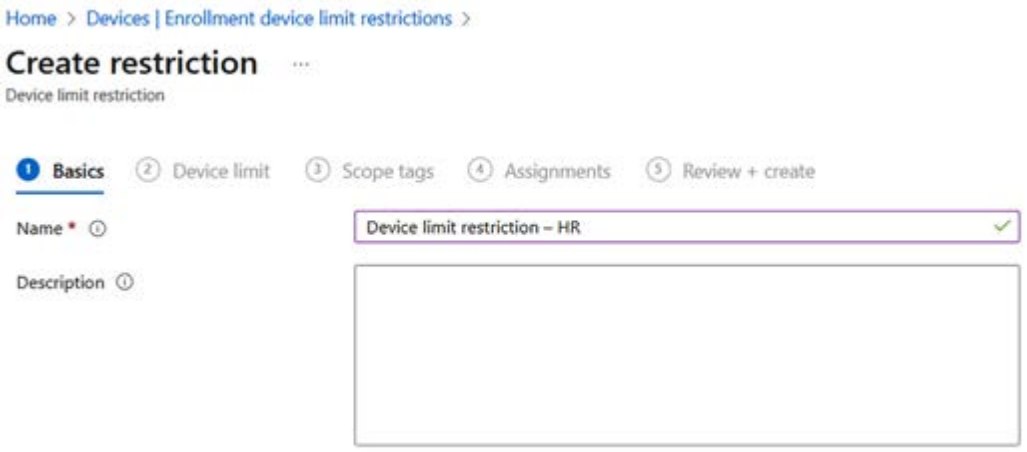


Figure 3.21: Microsoft Intune admin center – Device limit restriction

2. You can set **Device limit** to a number from `1` to `15`. The default in Microsoft Intune is a limit of `5`:

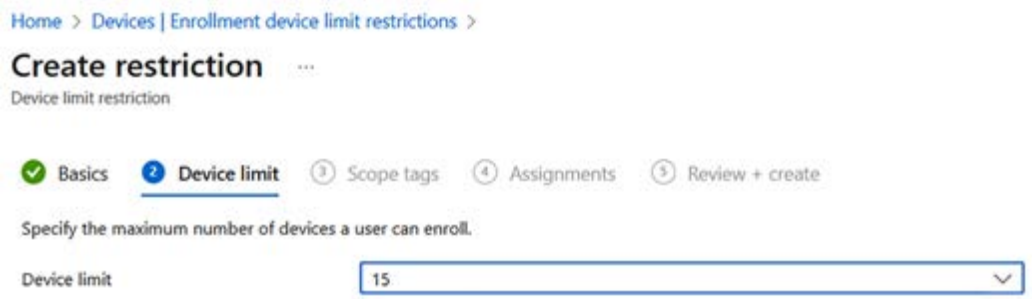


Figure 3.22: Microsoft Intune admin center – Device limit restriction

3. For the **Assignments** step, select **HR Department.**

   When you are creating a custom enrollment restriction, you can scope it to apply to specific user groups in your organization, departments, countries, and so on:

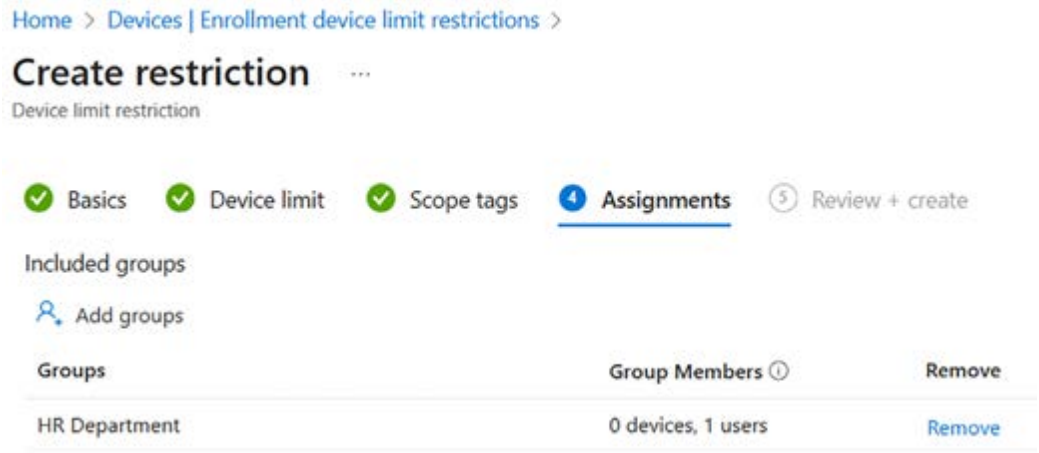


Figure 3.23: Microsoft Intune admin center – Device limit restriction – Assignments

4. In the following screenshot, you can see an overview of the default device limit restrictions.



Figure 3.24: Microsoft Intune admin center – Enrollment restriction – an overview

If you have *restricted personal enrollment*, your end users will be met with the **Something went wrong** screen if the devices are Entra joined and the devices are not in the Windows Autopilot service:

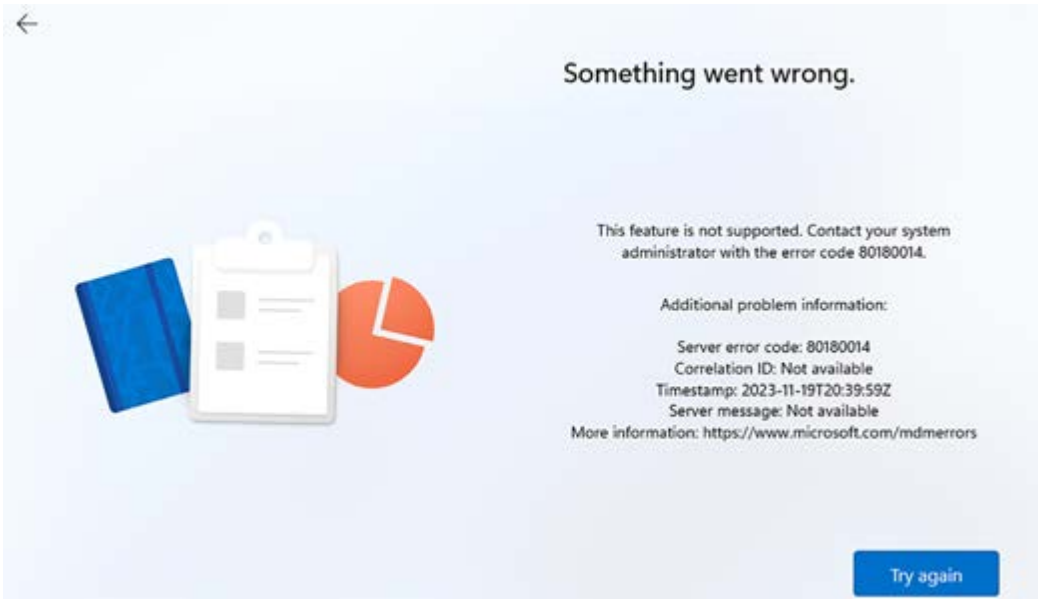


Figure 3.25: Windows 11 – an OOBE error

In the **Something went wrong** screenshot, note the error code **80180014**; this means that you are blocked from MDM enrolling your devices. However, as you have configured automatic MDM enrolment for your devices, Intune enrolment restriction will cover you here and ensure that your end users are only able to enrol corporate-owned Windows devices. If the error message came from Entra ID when joining the device, it would have been a different message.

Now that we have looked at different ways to restrict device enrollment in Microsoft Intune, we will look at the company branding of Microsoft Intune in the next section.

Customizing Intune Company Portal apps, the Company Portal website, and the Intune app

Company branding in Intune allows an IT administrator to control the look and feel of the Intune Company Portal, which is a web-based portal or an application that allows end users to access company resources and applications from their devices. We will now show you how you, as an IT admin, can customize the Company Portal:

1. Go to **Tenant administration.** Click on **Customization** | **Settings** | **Edit**:



NOTE

This is the default customization that's applied to all users and devices. It can be edited but not deleted.

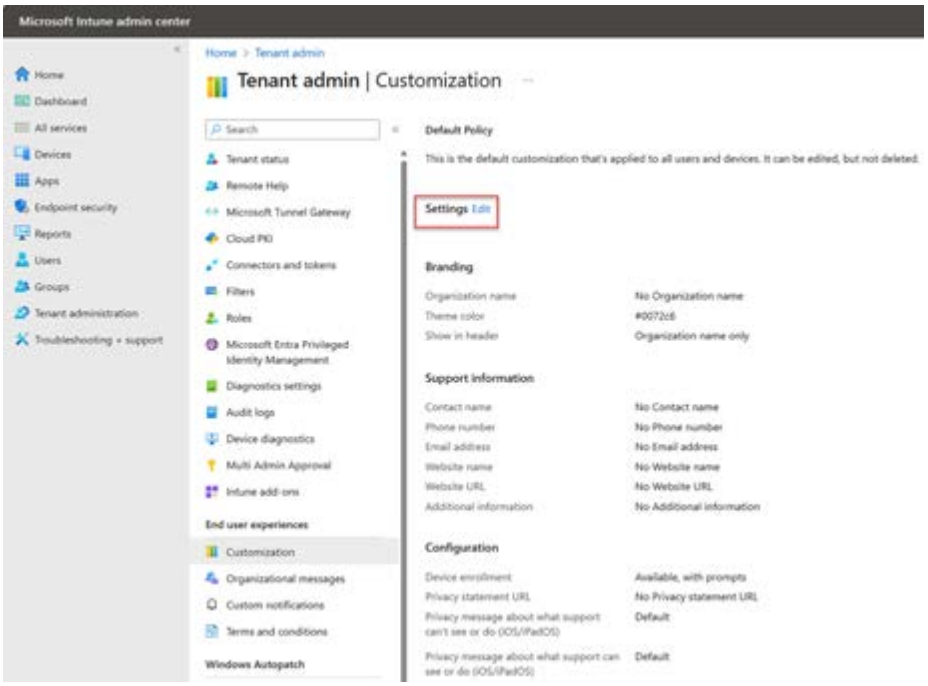


Figure 3.26: Admin portal – Customization

2. Create branding for your organization's Entra sign-in page:

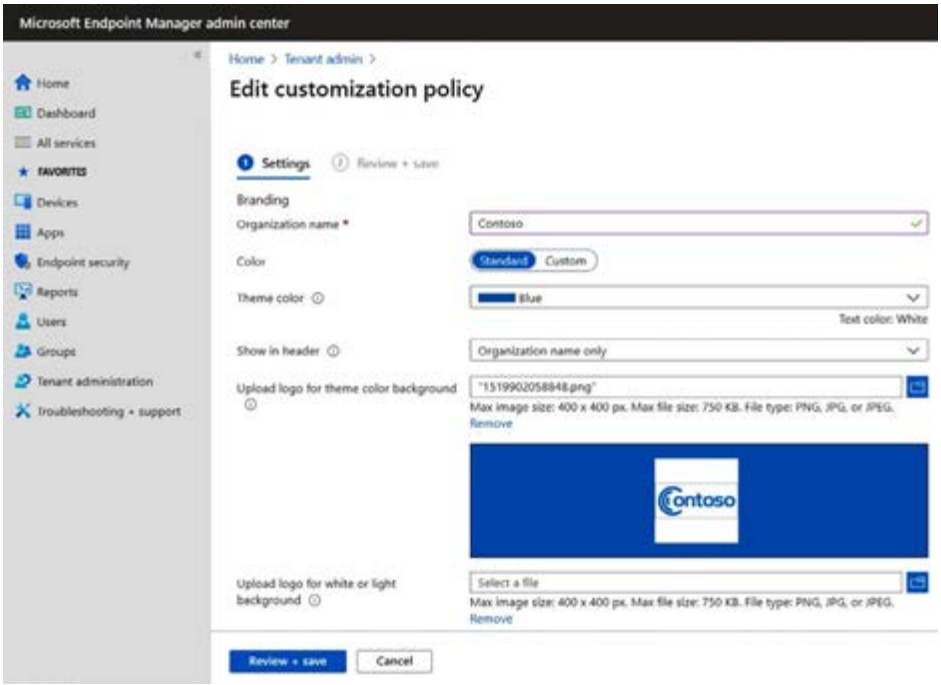


Figure 3.27: Admin portal – Customization

3. If you set **Color** as **Custom**, you have the option to use hex color codes to match the exact color that your company uses in its digital marketing:



Figure 3.28: Admin portal – Customization

App Sources is where you choose which additional app sources will be shown in the Company Portal:

- Entra Enterprise applications
- Office Online applications

You can use the hide features to prevent or allow users from performing self-service actions on devices in the Company Portal website and client apps.

The following actions are available:

- Hide the remove button on corporate Windows devices.
- Hide the reset button on corporate Windows devices.
- Hide the remove button on corporate iOS/iPadOS devices.
- Hide the reset button on corporate iOS/iPadOS devices.

You can create a customization policy and assign it to select groups in your organization. When assigned, this type of policy overrides the default policy. If you assign more than one of these policies to a user, the user will get the first policy you created.

You can create a maximum of 10 customization policies in your Microsoft Intune tenant.

The Company Portal is a self-service app for the end user to get apps from Microsoft Intune, Microsoft Store for Business, Entra Enterprise apps, Office Online applications, web link, and Configuration Manager apps (if the device is in a co-management state):

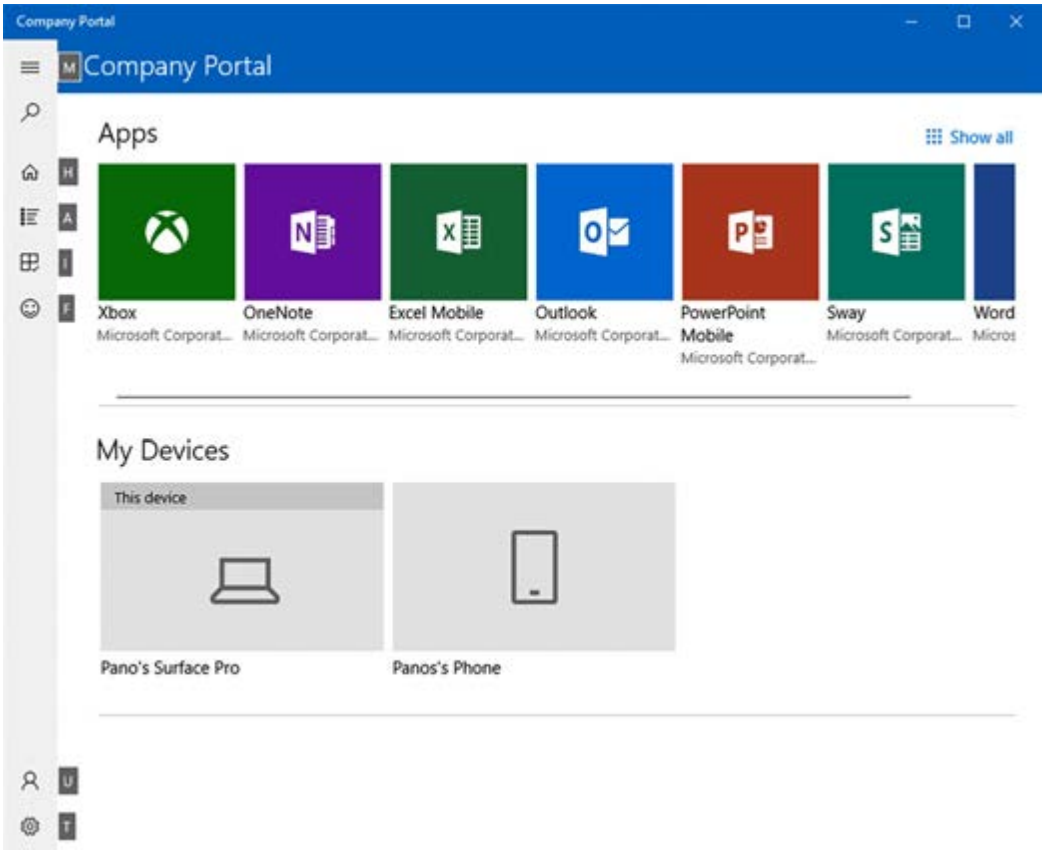


Figure 3.29: Company Portal – example

We have covered the branding part of Microsoft Intune in this section. In the next section, we will cover the network URL requirement for Intune.

Microsoft Intune – network URL firewall requirements

The table in this section lists the URLs and port settings that you are required to have full access to, from both your physical endpoint location as well as on Azure. You can find the full list of all the required Microsoft Intune URLs here: `aka.ms/microsoftintuneURLs`.



NOTE

Are you using Intune in China? Make sure to open the right level of network access via Intune, operated by 21Vianet in China | Microsoft Docs: `https://learn.microsoft.com/en-us/mem/intune/fundamentals/china`.

Access for managed devices

The following table lists the domains to provide access for managed devices:

FQDN	Associated Service
*.manage.microsoft.com	Intune service
manage.microsoft.com	Intune service
*.prod.do.dsp.mp.microsoft.com	Windows Update and Delivery Optimization
*.windowsupdate.com	Windows Update and Delivery Optimization
*.dl.delivery.mp.microsoft.com	Windows Update and Delivery Optimization
*.update.microsoft.com	Windows Update and Delivery Optimization
*.delivery.mp.microsoft.com	Windows Update and Delivery Optimization
tsfe.trafficshaping.dsp.mp.microsoft.com	Windows Update and Delivery Optimization
emdl.ws.microsoft.com	Delivery Optimization
*.do.dsp.mp.microsoft.com	Delivery Optimization
*.emdl.ws.microsoft.com	Delivery Optimization
*.notify.windows.com	Push notifications
*.wns.windows.com	Push notifications
devicelistenerprod.microsoft.com	Windows Update for Business deployment service
devicelistenerprod.eudb.microsoft.com	Windows Update for Business deployment service
login.windows.net	Windows Update for Business deployment service
payloadprod*.blob.core.windows.net	Windows Update for Business deployment service
time.windows.com	NTP sync
www.msftconnecttest.com	NTP sync
www.msftncsi.com	NTP sync
*.s-microsoft.com	Windows notifications and store
clientconfig.passport.net	Windows notifications and store
windowsphone.com	Windows notifications and store
approdimedatahotfix.azureedge.net	Scripts and Win32 apps
approdimedatapri.azureedge.net	Scripts and Win32 apps
approdimedatasec.azureedge.net	Scripts and Win32 apps
euprodimedatahotfix.azureedge.net	Scripts and Win32 apps
euprodimedatapri.azureedge.net	Scripts and Win32 apps

euprodimedatasec.azureedge.net	Scripts and Win32 apps
naprodimedatahotfix.azureedge.net	Scripts and Win32 apps
naprodimedatapri.azureedge.net	Scripts and Win32 apps
swda01-mscdn.azureedge.net	Scripts and Win32 apps
swda02-mscdn.azureedge.net	Scripts and Win32 apps
swdb01-mscdn.azureedge.net	Scripts and Win32 apps
swdb02-mscdn.azureedge.net	Scripts and Win32 apps
swdc01-mscdn.azureedge.net	Scripts and Win32 apps
swdc02-mscdn.azureedge.net	Scripts and Win32 apps
swdd01-mscdn.azureedge.net	Scripts and Win32 apps
swdd02-mscdn.azureedge.net	Scripts and Win32 apps
swdin01-mscdn.azureedge.net	Scripts and Win32 apps
swdin02-mscdn.azureedge.net	Scripts and Win32 apps
ekcert.spserv.microsoft.com	Autopilot self-deploy
ekop.intel.com	Autopilot self-deploy
ftpm.amd.com	Autopilot self-deploy
*.itunes.apple.com	Apple device management
*.mzstatic.com	Apple device management
*.phobos.apple.com	Apple device management
5-courier.push.apple.com	Apple device management
ax.itunes.apple.com.edgesuite.net	Apple device management
itunes.apple.com	Apple device management
ocsp.apple.com	Apple device management
phobos.apple.com	Apple device management
phobos.itunes-apple.com.akadns.net	Apple device management
intunecdnpeasd.azureedge.net	Intune - Android AOSP Dependency
*.channelservices.microsoft.com	Remote Help
*.go-mpulse.net	Remote Help
*.infra.lync.com	Remote Help
*.resources.lync.com	Remote Help
*.support.services.microsoft.com	Remote Help
*.trouter.skype.com	Remote Help

*.vortex.data.microsoft.com	Remote Help
edge.skype.com	Remote Help
remoteassistanceprodacs.communication.azure.com	Remote Help
lgmsapeweu.blob.core.windows.net	Collect diagnostics
fd.api.orgmsg.microsoft.com	Organizational messages
ris.prod.api.personalization.ideas.microsoft.com	Organizational messages
contentauthassetscdn-prod.azureedge.net	Organizational messages
contentauthassetscdn-prodeur.azureedge.net	Organizational messages
contentauthrafcontentcdn-prod.azureedge.net	Organizational messages
contentauthrafcontentcdn-prodeur.azureedge.net	Organizational messages

Table 3.1: Domains

Network requirements for PowerShell scripts and Win32 apps

If you're using Intune to deploy PowerShell scripts or Win32 apps, you'll also need to grant access to endpoints in which your tenant currently resides.

To find your tenant location (or **Azure Scale Unit** (**ASU**)), go through the following steps:

1. Sign in to the Microsoft Intune admin center.
2. Go to **Tenant administration** | **Tenant details**.

   The location can be found under **Tenant location** as something such as **North America 0501** or **Europe 0202**. Look for the matching number in the following table.

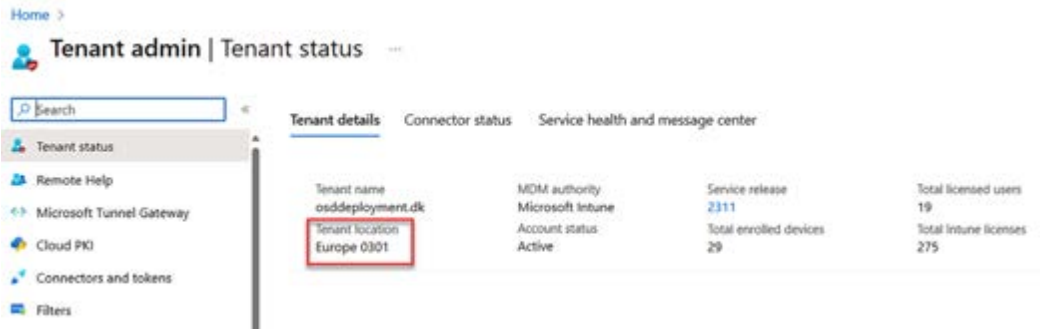


Figure 3.30: Tenant location

The rows are differentiated by geographic region, as can be seen in the first two letters in the names (**eu = Europe**, **na = North America**, and **ap = Asia Pacific**). Although your organization's actual geographic location might be elsewhere, your tenant location will be one of these three regions:

Azure Scale Unit (ASU)	Storage name	CDN
AMSUA0601 AMSUA0602 AMSUA0101 AMSUA0102 AMSUA0201 AMSUA0202		
AMSUA0401	naprodimedatapri	naprodimedatapri.azureedge.net
AMSUA0402	naprodimedatasec	naprodimedatasec.azureedge.net
AMSUA0501	naprodimedatahotfix	naprodimedatahotfix.azureedge.net
AMSUA0502 AMSUA0601 AMSUA0701 AMSUA0702 AMSUA0801 AMSUA0901		
AMSUB0101 AMSUB0102 AMSUB0201 AMSUB0202		
AMSUB0301	euprodimedatapri	euprodimedatapri.azureedge.net
AMSUB0302	euprodimedatasec	euprodimedatasec.azureedge.net
AMSUB0501	euprodimedatahotfix	euprodimedatahotfix.azureedge.net
AMSUB0502 AMSUB0601 AMSUB0701		

AMSUC0101 AMSUC0201 AMSUC0301 AMSUC0501 AMSUC0601 AMSUD0101	approdimedatapri approdimedatasec approdimedatahotifx	approdimedatapri.azureedge.net approdimedatasec.azureedge.net approdimedatahotfix.azureedge.net

Table 3.2: Regions

Microsoft Store endpoint URLs

Intune-managed Windows devices using the Microsoft Store – either to install or update apps – will need access to these endpoints. Some Win32 apps from the store have their binaries stored at the **Independent Software Vendor** (**ISV**), * such as Adobe Acrobat Reader, which is not stored in the Microsoft Store URLs, and you need to check with each ISV where they store their apps.

Microsoft Store API (`AppInstallManager`):

- `displaycatalog.md.mp.microsoft.com`
- `purchase.md.mp.microsoft.com`
- `licensing.mp.microsoft.com`
- `storeedgefd.dsx.mp.microsoft.com`

Windows 365 endpoint URLs

Please whitelist traffic to the following URLs when using cloud PC endpoints:

- `cpcsacnrysa1prodprna02.blob.core.windows.net`
- `cpcsacnrysa1prodprap01.blob.core.windows.net`
- `cpcsacnrysa1prodprau01.blob.core.windows.net`
- `cpcsacnrysa1prodpreu01.blob.core.windows.net`
- `cpcsacnrysa1prodpreu02.blob.core.windows.net`
- `cpcsacnrysa1prodprna01.blob.core.windows.net`

Windows Push Notification Services – required URLs

The **Windows Push Notification Services** (**WNS**) enable Microsoft Intune to send toast, tile, badge, and raw updates from the Microsoft Intune cloud service to Windows clients:

- `*.notify.windows.com`
- `*.wns.windows.com`
- `*.notify.live.net`
- `login.microsoftonline.com`
- `login.live.com`

Windows 365 and Azure Virtual Desktop – required URLs

The Azure VMs you create for Windows 365 and Azure Virtual Desktop must have outbound TCP 443 access to the following URLs via the required Azure virtual network in the customer's Azure subscription. You can find the full list of all the required Azure Virtual Desktop URLs here: `aka.ms/CPCURLs`.

More information about the requirements for Windows 365 can be found in the previous chapter.

You can find a list of all the URLs per service purpose in the following table:

Address	Outbound TCP Port	Purpose
*.wvd.microsoft.com	443	Service traffic
gcs.prod.monitoring.core.windows.net	443	Agent traffic
production.diagnostics.monitoring.core.windows.net	443	Agent traffic
*xt.blob.core.windows.net	443	Agent traffic
*eh.servicebus.windows.net	443	Agent traffic
*xt.table.core.windows.net	443	Agent traffic
catalogartifact.azureedge.net	443	Azure Marketplace
kms.core.windows.net	1688	Windows activation
mrsglobalsteus2prod.blob.core.windows.net	443	Agent and SXS stack updates
wvdportalstorageblob.blob.core.windows.net	443	Azure portal support
169.254.169.254	80	Azure Instance Metadata Service endpoint(`https:docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service`)
168.63 .129.16	80	Session host health monitoring (`https:docs.microsoft.com/en-us/azure/virtual-network/security-overview`)

Table 3.3: URLs

Universal Print – required URLs

A Windows endpoint that is used with Universal Print needs to have an internet connection, with access to the following internet (TCP/IP – 443) endpoints:

- `*.print.microsoft.com`
- `*.microsoftonline.com`
- `*.azure.com`

- *.msftauth.net
- go.microsoft.com
- aka.ms

Delivery Optimization

For peer-to-peer traffic, Delivery Optimization uses 7680 for TCP/IP or 3544 for NAT traversal (optionally Teredo). For client-service communication, it uses HTTP or HTTPS over port 80/443.

Delivery Optimization will help with band-wide consumption on Windows endpoints:

- *.do.dsp.mp.microsoft.com
- *.dl.delivery.mp.microsoft.com
- *.emdl.ws.microsoft.com

Summary

In this chapter, you've learned about the different supported endpoint scenarios within Microsoft Intune and what the requirements are to use the service.

In the next chapter, we're going to take a deeper dive into how to deploy Windows Enterprise to your endpoints. We're also going to discuss Autopilot and how this deployment service can deliver out-of-the-box configurations for your physical endpoints!

Questions

1. What is the minimum set of privileges to have to configure Microsoft Intune?
    a. Global Admin
    b. Azure Owner
    c. Intune Administrator
2. What is the menu option called in Microsoft Intune that changes the branding and logos as part of your organization?
    a. Tenant admin
    b. Customization
    c. Tenant administration
3. What should be the required Entra configuration to use Windows 365 and Azure Virtual Desktop?
    a. Entra
    b. Entra Domain Services
    c. Entra hybrid joined

Answers

1. (c)
2. (b)
3. (c)

Further reading

If you want to learn more about Microsoft Intune requirements after reading this chapter, please use the following free online resources:

- *Network endpoints for Microsoft Intune | Microsoft Docs*: `https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-endpoints`
- *OSes and browsers supported by Microsoft Intune | Microsoft Docs*: `https://learn.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers`
- *Intune operated by 21Vianet in China | Microsoft Docs*: `https://learn.microsoft.com/en-us/mem/intune/fundamentals/china`
- *Network requirements and bandwidth details for Microsoft Intune | Microsoft Docs*: `https://learn.microsoft.com/en-us/mem/intune/fundamentals/network-bandwidth-use`

Get This Book's PDF Version and Exclusive Extras

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

***Note**: Keep your invoice handy. Purchases made directly from Packt don't require one.*



Section II

Windows 365

In this section, you'll learn everything you need to know about the new cloud service Windows 365. As this service has just been released, we decided to dedicate a full section on it, to allow you to kick the tires.

This part of the book comprises the following chapters:

- *Chapter 4*, *What Is Windows 365?*
- *Chapter 5*, *Deploying Windows 365*

4

What is Windows 365?

In this chapter, you'll learn everything you need to know about Windows 365 from a conceptual perspective.

After reading this chapter, you'll know more about the benefits of using Windows 365 and the different service components. In the next chapter, you'll learn how you can deploy it!

This chapter is very comprehensive – we'll go through the following topics:

- What is Windows 365?
- Removing the complexity of traditional **Virtual Desktop Infrastructure** (**VDI**) deployments
- What to think about as a VDI administrator
- Windows 10 **Extended Security Updates** (**ESUs**)
- Comparing Windows 365 Enterprise and Business
- What is Windows 365 Frontline?
- What is Windows 365 Government?
- Microsoft Intune
- Configuration Manager support
- Co-management and Windows 365
- Disaster recovery
- Sizes and performance of fixed-price licenses
- GPU-Enhanced Cloud PCs
- Connect to your on-premises network
- Provisioning policies
- Windows 365 – gallery images
- Custom images
- Windows Updates via Autopatch
- Roles and delegation

- The Watchdog service
- Optimized Teams on Windows 365
- Screen capture protection and watermarking

What is Windows 365?

Users want technology that is familiar, easy to use, and always available so they can work and create Office and other business-related content fluidly across devices. Cloud PCs make this possible by combining the power and security of the cloud with the familiarity of a PC. Only Microsoft can bring together a PC, Microsoft Intune, and the cloud with a consistent and integrated Windows experience. Windows 365 is the world's first Cloud PC. With Windows 365 Cloud PC, Windows evolves from a device-based **Operating System** (**OS**) to hybrid personalized computing that you can run from different platforms, like iPads and smartphones, via the new Windows app that is now available from almost any platform.

> *"With Windows 365, we're creating a new category: the Cloud PC. Just like applications were brought to the cloud with SaaS, we are now bringing the operating system to the cloud..."* – **Satya Nadella**, *CEO, Microsoft*

During the launch of Windows 365 back in July 2021, Microsoft CEO, Satya Nadella, shared a quote about bringing Windows to the Cloud, blurring the lines between Windows today and in the future. The vision that outlined a rich set of features has also been explained by our senior leaders who contributed to the foreword of this book.

Windows 365 delivers Cloud PCs, a complete and secure Windows experience hosted in the Microsoft Cloud and accessible on any device. Whether your employees are full-time or contractors, shift workers, or seasonal staff, they can access their personalized Windows apps, settings, desktops, and data on the device of their choice and from wherever they work. Windows 365 Cloud PCs help enable **Bring your own PC** (**BYOPC**) programs, onboard employees within minutes, reduce management and security headaches, and ensure your workforce is always up and running. With Microsoft Entra ID and Microsoft Intune, Cloud PCs are easy to configure, deploy, manage, and secure, so you can maximize existing technology resources to meet the needs of all your employees.

You can find all the main principles of the service in the following list:

- Deploy and manage virtual endpoints in Microsoft Intune; no additional VDI expertise or resources are needed.
- Procure, provision, and deploy in minutes, with optional automated OS updates.
- Access from anywhere to your personalized Windows desktop experience.
- Tailor compute and configurations for an elastic workforce.

- Pick up where you left off on the device of your choice.
- Optimized experiences on Windows endpoints.
- Scale confidently with per-user pricing.

Removing the complexity of traditional VDI deployments

All the building blocks are automated for you, and the service scales with you in the most optimized way possible to use Microsoft 365 apps. It is Microsoft's best expression of Windows and Microsoft 365 and is always secure and up to date.

A Cloud PC can be accessed from anywhere from any device and can scale with a user's changing compute needs, meaning that the user could receive the self-service privileges to release an IT admin from needing to assign a license that provides more compute resources. The same applies to storage upgrades and Cloud PC reboots – more about this later.

What to think about as a VDI administrator

If you're using any virtualization solution right now with OneDrive, we recommend you enable the OneDrive Known Folder Move feature. This allows you to synchronize the user's desktop, pictures, videos, and documents to OneDrive. Windows 365 supports the OneDrive Known Folder Move feature out of the box, so the first time the user logs on, the files will be there.

Windows 365 uses local profiles only to remove the complexity of profile management solutions such as the FSLogix profile container. Cloud PCs are persistent, personal, and dedicated to the user. It's replicated across multiple zones in an Azure region and automated restore points to make the profile high availability as part of the service.

Leverage Microsoft Edge for Business so that your personal browser history and settings are roaming between Microsoft Edge on different platforms, including Windows 365 Cloud PCs.

Enterprise State Roaming is used to roam Windows settings. Enable this in your Entra ID tenant settings to ensure your Windows Personalization settings are also coming over!

Removing complexity while increasing security

Windows 365 removes the complexity of management as well as the end user experience while also adding a higher security level to your endpoints, as the remote desktop protocol ensures an always encrypted connection from the endpoint to the Cloud PC that never leaves data behind on the endpoint – all the Cloud PCs are also encrypted on the disk level. The service is fully supported by Microsoft Defender for Endpoints and Zero-Trust principles, with enhancements for Entra ID conditional access rules – securing your virtual desktops has never been easier to configure.

Low costs as a fixed-price model

The other great benefits are the costs involved as this Windows 365 service could decrease the current cost of keeping your VDI environment up and running or any other use case; for example, remote workers connecting via an expensive, unreliable VPN connection. Windows 365 includes all the services you need end-to-end via Microsoft Intune.

It allows you to consolidate IT management processes in Intune to combine expertise in modern management for both physical and Cloud PCs. All the services are built using a subscription-based model that aligns with the CapEx needs of most businesses, too.

The following comparison model perfectly shows the differences between traditional Remote Desktop Services (session-based) and VDI, and **Azure Virtual Desktop** (**AVD**) and Windows 365:

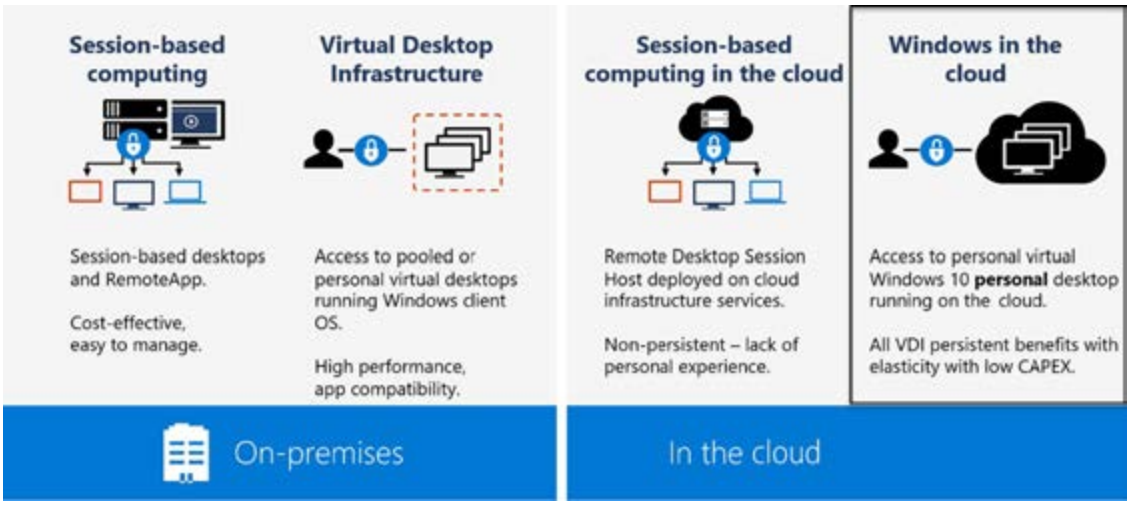


Figure 4.1: Comparison between an on-premises and Windows in the loud environment

Windows 365 is a fixed-price service with a personal Windows experience completely managed via Microsoft Intune.

The transition to modern management with Microsoft Intune

Microsoft Intune is an integrated solution that simplifies management across multiple OSs, cloud, on-premises, mobile, desktop, and virtualized endpoints including Cloud PCs, and it lowers the **Total Cost of Ownership** (**TCO**). It empowers organizations to provide data protection and endpoint compliance that supports a Zero-Trust security model. This unified management tool brings together device visibility, endpoint security, and data-driven insights to increase IT efficiency and improve user experiences in any work environment.

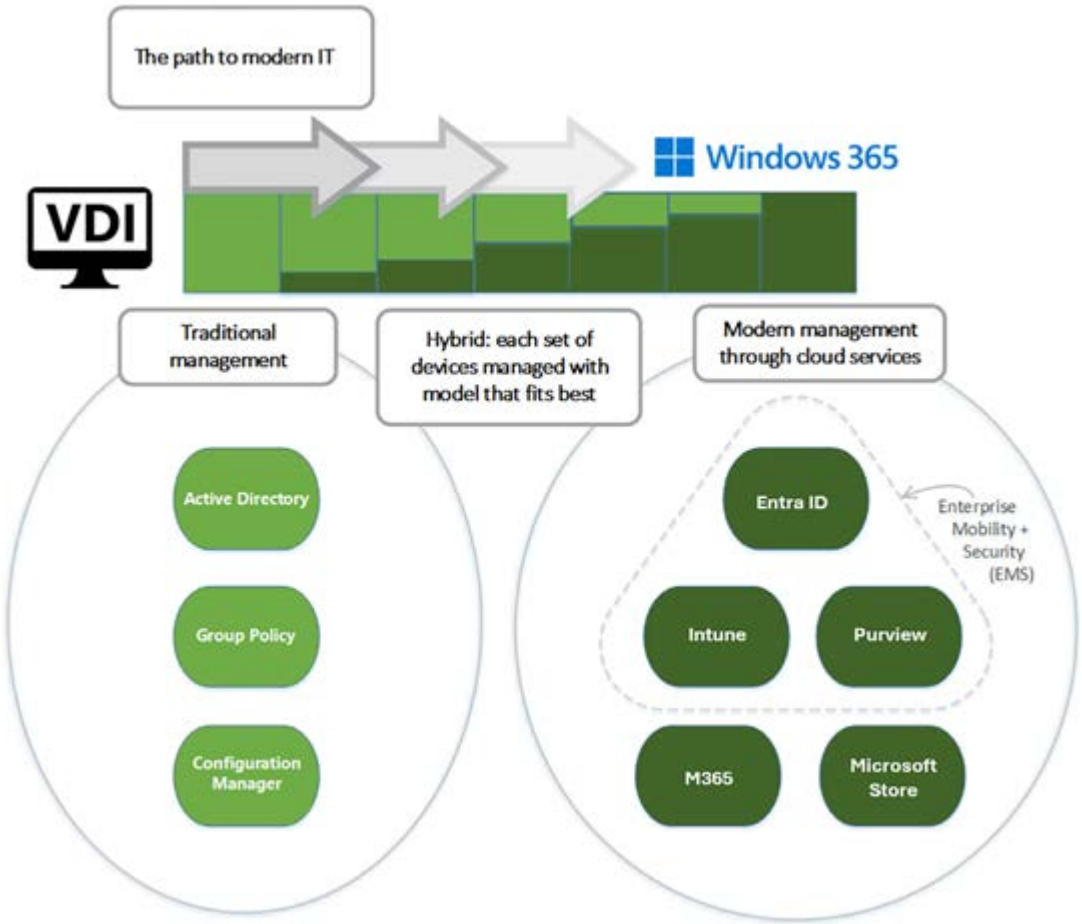


Figure 4.2: The path to modern IT

Windows 10 ESUs

As you work on modernizing your endpoint estate, you can move workers with Windows 10 PCs to Windows 11 in the cloud with Windows 365. That way, your employees will always be updated with the latest Windows 11 and the latest security protection available.

Windows 365 subscriptions will include ESUs at no additional cost for Windows 10 devices that access and use it in conjunction with Windows 365.

You might have scenarios in your organization where you're looking for options and the flexibility to continue using older Windows 10 PCs longer. Extending the life of Windows 10 PCs with ESUs and Windows 365 becomes a real possibility to support certain worker cohorts and still migrate to Windows 11. You can extend the life of these devices for an additional 3 years.

Windows 365 recently made a new service option generally available for frontline and shift workers. If workers don't use a dedicated personal computer but rather use a device that is shared or an older device, they can access Windows 11 using Windows 365. In these scenarios, you can extend the use of older Windows 10 PCs.

Comparing Windows 365 Enterprise and Business

Windows 365 is available in two versions, one fully managed and configurable via Microsoft Intune (mostly covered in this book) called **Windows 365 Enterprise**, and one called **Windows 365 Business**, where you have to provide more services yourself, such as application delivery and management.

Customers can purchase Windows 365 Business directly from the Microsoft 365 admin center portal, set up their account without a domain, and provision and manage their Cloud PCs directly from the Windows 365 homepage online.

No other Microsoft licenses are required: you can get started with just a credit card if you want. Windows 365 Business is intended for customers wanting to deploy Cloud PCs for 300 users or fewer across their organization.

Windows 365 Business allows customers to start provisioning a Cloud PC directly after assigning the license to the user from the Microsoft 365 admin center. There is no IT admin interaction needed. The user will be able to access the Cloud PC and become productive in under an hour after the license has been assigned!

In the following table, you can find the list of features available per product to make your decision easier in each scenario:

Feature	Windows 365 Business	Windows 365 Enterprise
Domain join feature	Entra ID join without Azure **Virtual Network** (**VNet**) support.	Entra ID Join without VNet support. Entra ID Join with VNet support. Hybrid Entra ID with VNet support.
Purchase channel support	Microsoft 365 Admin Center or the Entra ID portal.	Microsoft 365 Admin Center or the Entra ID portal.
License portal	No licensing pre-requirements to buy and deploy Windows 365 Business. Other features (like device management) can be used if users are licensed for Microsoft Endpoint Management.	Each user must be licensed for Windows 10 or 11 Enterprise (when available), Microsoft Intune, and Entra ID P1.

Networking costs	Outbound data/month is based on the RAM of the Cloud PC: - 2-GB RAM = 12-GB outbound data - 4-GB or 8-GB RAM = 20-GB outbound data - 16-GB RAM = 40-GB outbound data - 32-GB RAM = 70-GB outbound data Data bandwidth may be restricted when these levels are exceeded.	When providing a network, Networking goes through the customer's Azure VNet and isn't included in the license. Azure bandwidth pricing applies to these network usage costs. If using a Microsoft-hosted network, the same charges (as described in Windows 365 Business networking charges) apply.
Seat limit	300 seats per tenant.	No limits
Provisioning	Provisioning is simplified and uses default configurations. Cloud PCs are automatically provisioned with a standard image after a Cloud PC license is assigned.	Provisioning is configurable and customizable to the needs of the organization. Administrators select the network, configure user permissions (local admin or not), and assign the policy to an Entra ID group. Cloud PCs are then provisioned by using standard gallery images or custom images (admin choice).
Policy management	Not supported.	**Group Policy Objects** (**GPOs**) and Intune MDM are supported.
Monitoring	Not supported.	Endpoint analytics reporting and monitoring, service health, and operational health alerts.
Universal Print	Universal Print.	Universal Print.
End user management	Users can restart, reset, rename, and troubleshoot their Cloud PCs on the Windows 365 homepage.	Users can restart, rename, and troubleshoot their Cloud PCs on the Windows 365 homepage.
Conditional Access	Conditional Access policies can be deployed only by using Entra ID with an Entra ID P1 license.	Conditional Access policies can be deployed by using the Microsoft Intune admin center or Entra ID.

Security baselines	Not supported.	Dedicated security baselines can be edited and deployed by using Microsoft Intune.
Microsoft Defender for Endpoint	Supported if the customer separately has the requisite E5 license.	Integration with Defender for Endpoint. If the customer has an E5 license, all Cloud PCs will respond to Defender for Endpoint policies and show up in MDE dashboards.

Table 4.1: Windows 365: Business and Enterprise

We're not covering Windows 365 Business explicitly in this book, however, there are many similarities as you have learned via the preceding table. The following screenshot shows the admin tool we introduced for our business product to maintain Cloud PCs in an efficient manner!

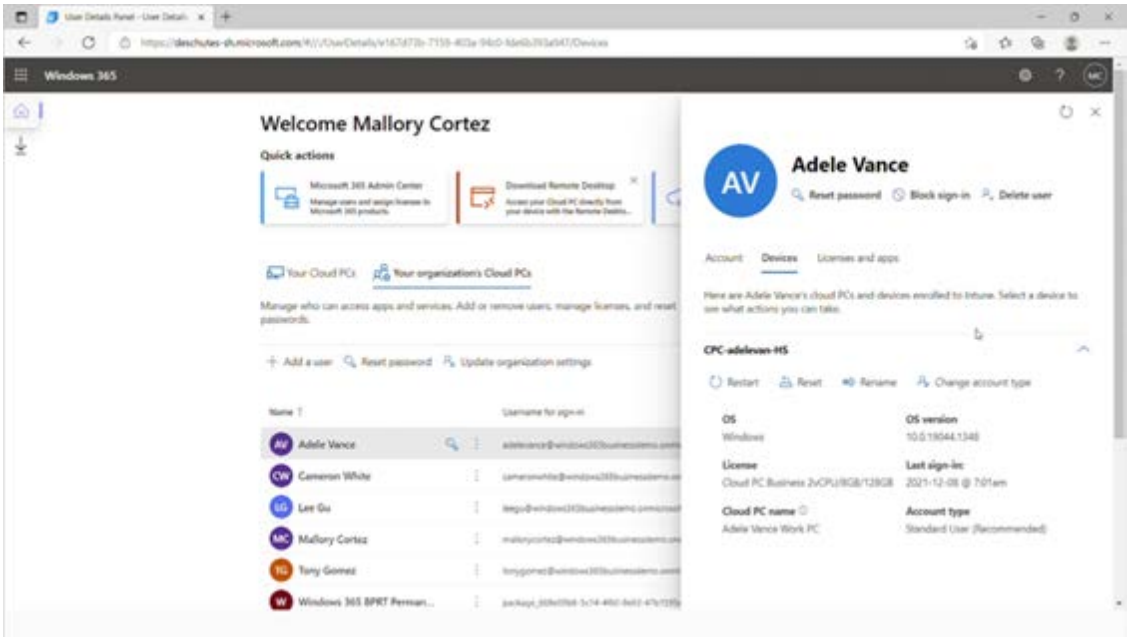


Figure 4.3: Windows 365 Business

We've now explained all the differences between the different products, so you can make the right decision as to whether Business or Enterprise is the better fit. Let's now switch over to Windows 365 Frontline.

What is Windows 365 Frontline?

Windows 365 Frontline is an exciting new offering that allows customers and shift workers the flexibility to provision Cloud PCs for up to three users with the purchase of a single license of Windows 365. In terms of feature stack, we want to bring a certain level of product parity across Windows 365 offerings. If you're coming from multi-session or server OS to Windows 365, this is an offering to investigate.

What is Windows 365 Government?

If you are looking for a cloud-based solution that meets the stringent compliance and security requirements of the US government, Windows 365 Government is the right choice for you. Windows 365 Government enables you to stream personalized Windows apps, data, content, and settings from a regulated US government cloud to any device at any time.

Windows 365 Government is designed for US federal, state, and local government agencies, as well as contractors who hold or process data on behalf of those agencies. It is available for customers who qualify to use services hosted in **Government Community Cloud** (**GCC**) and GCC High (supports FedRAMP High, ITAR, and DFARS) environments, which adhere to specific regulatory and audit standards. With Windows 365 Government, you can benefit from the flexibility, scalability, and security of the cloud while maintaining compliance with your data sovereignty and residency requirements.

Microsoft Intune

Windows 365 works together with Microsoft Intune, hence this book is named *Mastering Microsoft Intune*.

To configure Windows 365 from within the Microsoft Intune admin center in the **Devices** blade, you get access to Windows 365 – the Cloud PC service – where you can find the **Overview** dashboard screen showing the status of your environment:

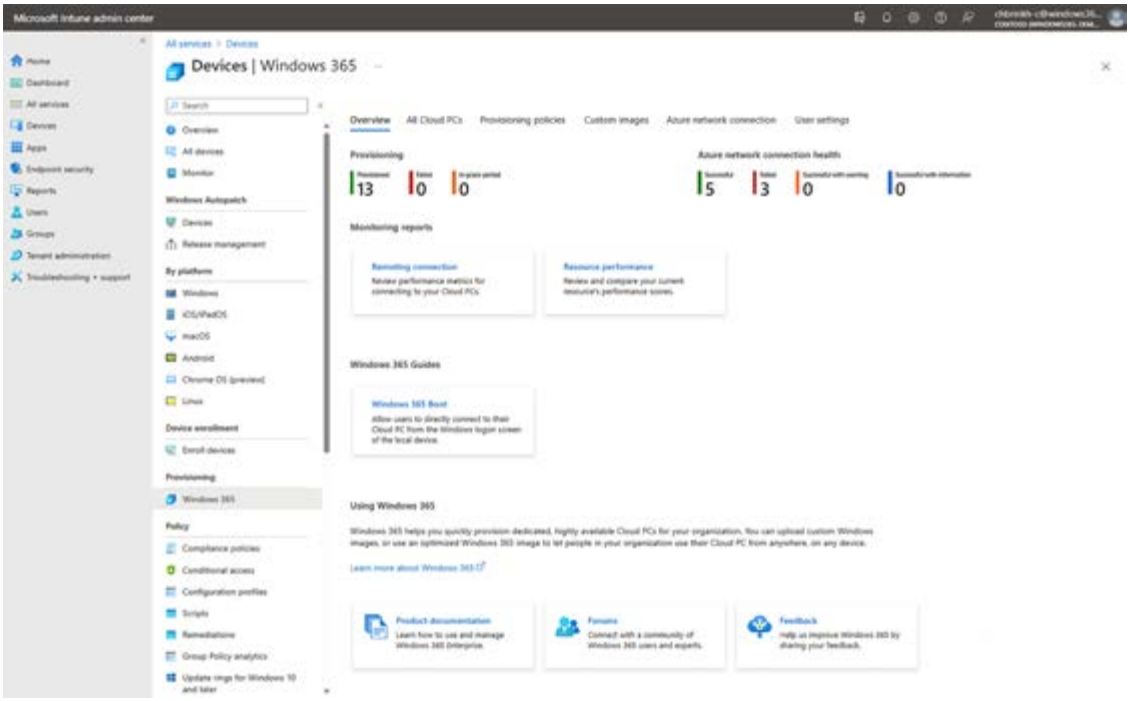


Figure 4.4: Overview dashboard

When you go to **Devices** in the menu and scroll down to **Provisioning**, you will find the spot to start creating your Cloud PCs with a provisioning policy:

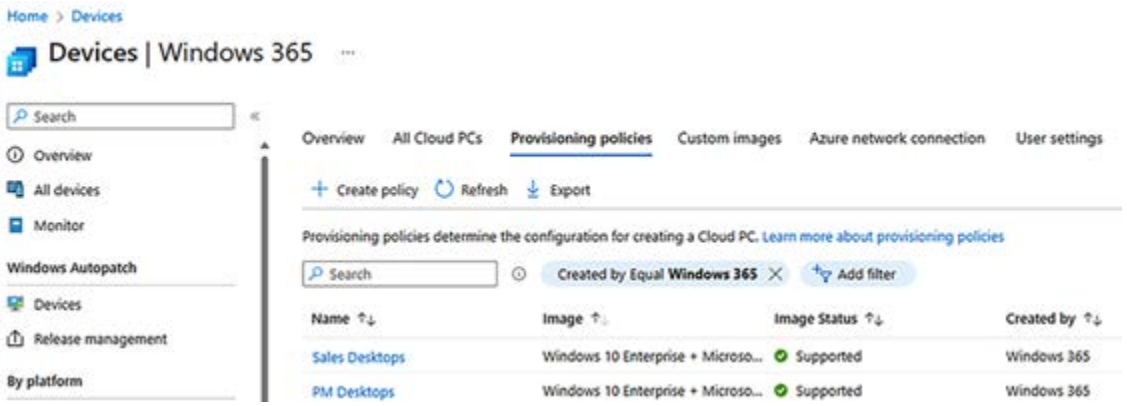


Figure 4.5: Provisioning Cloud PCs

All the prerequisite steps as well as the main steps to provision Cloud PCs are covered later in this chapter.

High-level architecture components and responsibilities

The architecture of Windows 365 is relatively simple to understand and a bit different from **AVD** as some objects now live in a Microsoft-managed environment.

In *Figure 6*, all the blue parts are now managed by Microsoft and the gray elements are the responsibility of the customer/partner. This is different from solutions where you are responsible for most things yourself, meaning more overhead in management and, most likely, a higher level of complexity.

Microsoft manages the following services as part of Windows 365:

- Virtualization control plane (information worker (web access) portal, gateway, connection broker, diagnostics, and REST APIs)
- Cloud PCs and Azure compute services (VMs, provisioning, Azure subscriptions, Cloud PC VM provisioning, autoscaling, and so on)

Customers and/or partners manage these components as part of Windows 365:

- Azure VNet (subnets, ExpressRoute, S2S VPN, and so on)
- Microsoft Intune (device configuration, settings catalog, PowerShell, and so on)
- Azure **Active Directory** (**AD**) configuration (hybrid Entra ID, Conditional Access, compliance policies, and so on)
- **Active Directory Domain Services** (**AD DS**) configuration (on-premises AD, Entra ID Connect, and so on)
- Physical endpoint clients (Windows, macOS, Linux, Android, iOS, and so on)

Microsoft Intune is the **unified management** console on top of all the other services we leverage, such as Entra ID, Defender for Endpoint, Endpoint analytics for monitoring, and Intune to manage your physical and cloud endpoints all at once.

The following diagram shows the high-level architecture of Windows 365 Enterprise with a hybrid Entra ID join as the domain configuration. It outlines the different responsibilities customers and partners have as part of the service as well as what other Microsoft Intune components are tightly integrated:

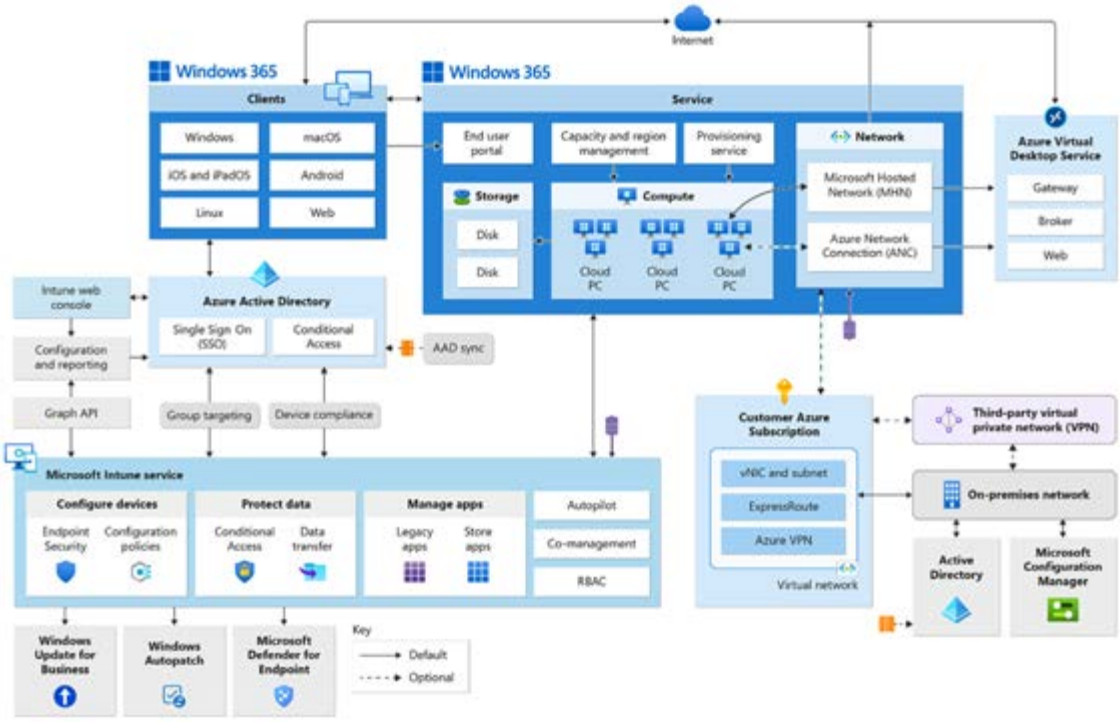


Figure 4.6: Microsoft Intune and Windows 365 architecture

You can download the preceding architecture drawing in high resolution via `https://learn.microsoft.com/en-us/windows-365/enterprise/high-level-architecture`.

Configuration Manager support

Configuration Manager is an on-premises management solution to manage desktops, servers, and laptops that are on your network or internet based. You can enable it to integrate with Intune, Entra ID, Microsoft Defender ATP, and other cloud services. Use Configuration Manager to deploy apps, software updates, and OSs. You can also monitor compliance, query, act on clients in real time, and much more.

Co-management and Windows 365

As part of Microsoft Intune, you can continue to use Configuration Manager as you always have. If you're ready to move some tasks to the cloud, consider co-management.

Co-management combines your existing on-premises Configuration Manager investment with the cloud using Intune and other Microsoft 365 cloud services. You choose whether Configuration Manager or Intune is the management authority for the seven different workload groups.

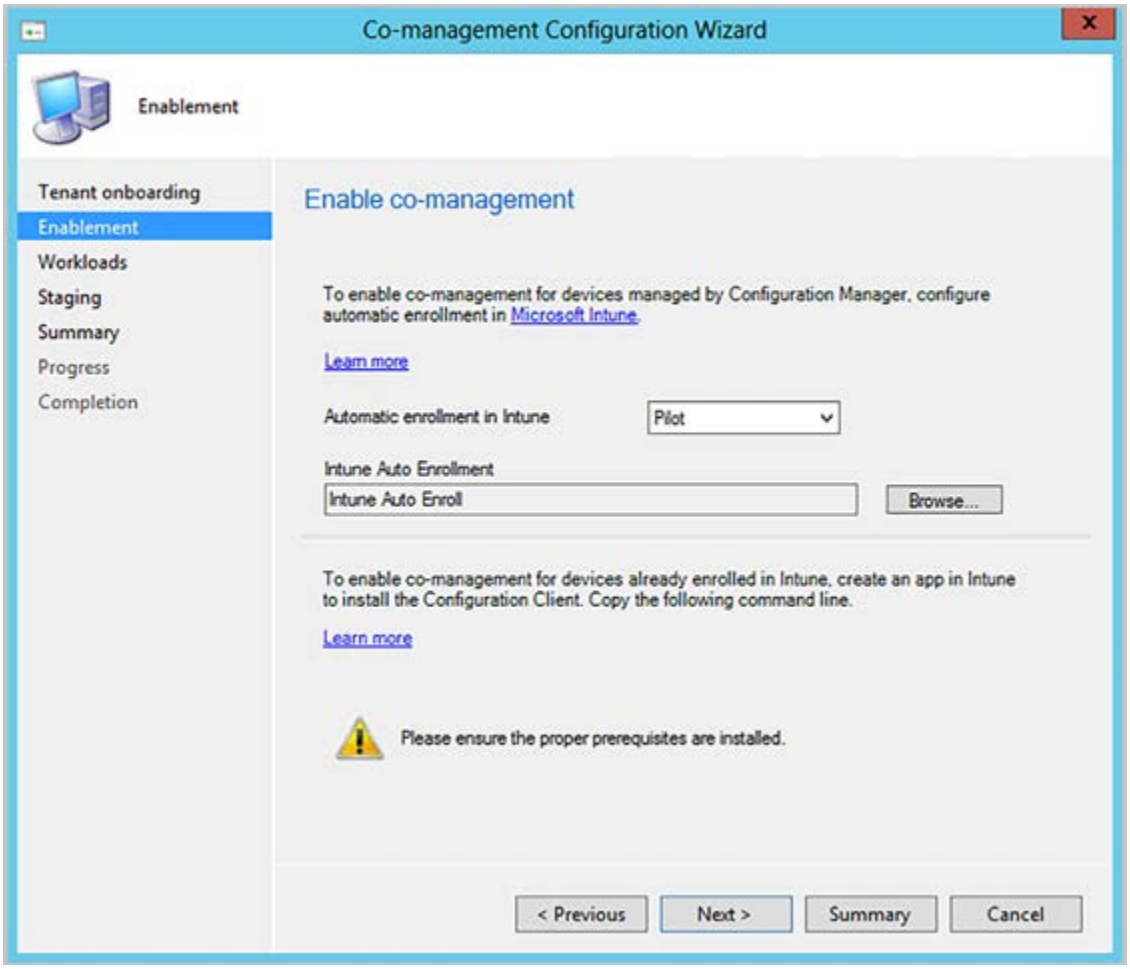


Figure 4.7: Enable co-management

Disaster recovery

Business continuity and disaster recovery (**BCDR**) are essential aspects of any organization's risk management strategy. Unexpected events, such as natural disasters, cyber-attacks, or other disruptions, can happen at any time, and without adequate planning and preparation, the impact can be devastating. Business continuity is the process of ensuring that vital business operations continue during a disruption, while disaster recovery is the process of restoring critical IT systems and infrastructure after an outage. Both are crucial for ensuring that organizations can bounce back quickly and minimize the damage of an unforeseen event.

As you know, BCDR can be a challenging task, especially when it comes to user desktops. Generally speaking, the process of business continuity planning involves four key aspects: assessment, planning, capability validation, and communication and coordination. Experts from various fields, such as compute, storage, applications, network, and user data, must collaborate to determine the best course of action in case of device, power, or network failures, among other things. After a plan is finalized, it can take several months or even years to build and test the system. Moreover, the process of executing a disaster recovery protocol can be stressful and complex, as it often requires quick and accurate implementation during times of high pressure and anxiety.

Windows 365, built on Microsoft's BCDR principles, offers highly reliable Cloud PCs with a financially backed **Service-Level Agreement** (**SLA**). If there is an in-zone Azure compute fabric failure, the Cloud PCs are automatically restored within a short **Recovery Time Objective** (**RTO**) of less than 10 minutes, and a **Recovery Point Objective** (**RPO**) that is almost zero. Windows 365 Cloud PCs are also designed to automatically recover from any underlying regional or zone failures, maintaining an RPO of approximately zero. This level of reliability gives customers the assurance that their critical data and operations will remain available, even in the face of unexpected disruptions.

Organizations can leverage Windows and Microsoft 365 solutions and features alongside Windows 365 to benefit from enhanced resilience of user data and context. Active/Active data resilience ensures that user data remains accessible through OneDrive, even during a Windows 365 outage. The automated disaster recovery process includes OneDrive, OneDrive for Business, and OneDrive with Known Folder Move, further enhancing the continuity of user data in the event of an outage. These features offer organizations a higher level of confidence in the resilience of their user data and context.

Windows 365 Cloud PCs are distributed across the zones within the region for each customer. Azure employs various techniques to ensure reliability within each zone, such as monitoring compute and seamlessly moving workloads to alternate resources within the zone in the event of disruption. Cloud PCs benefit from the reliability advantages provided to all Azure workloads. Furthermore, in the event of a zone failure, each Cloud PC can recover to a different zone within the same region that has available capacity.

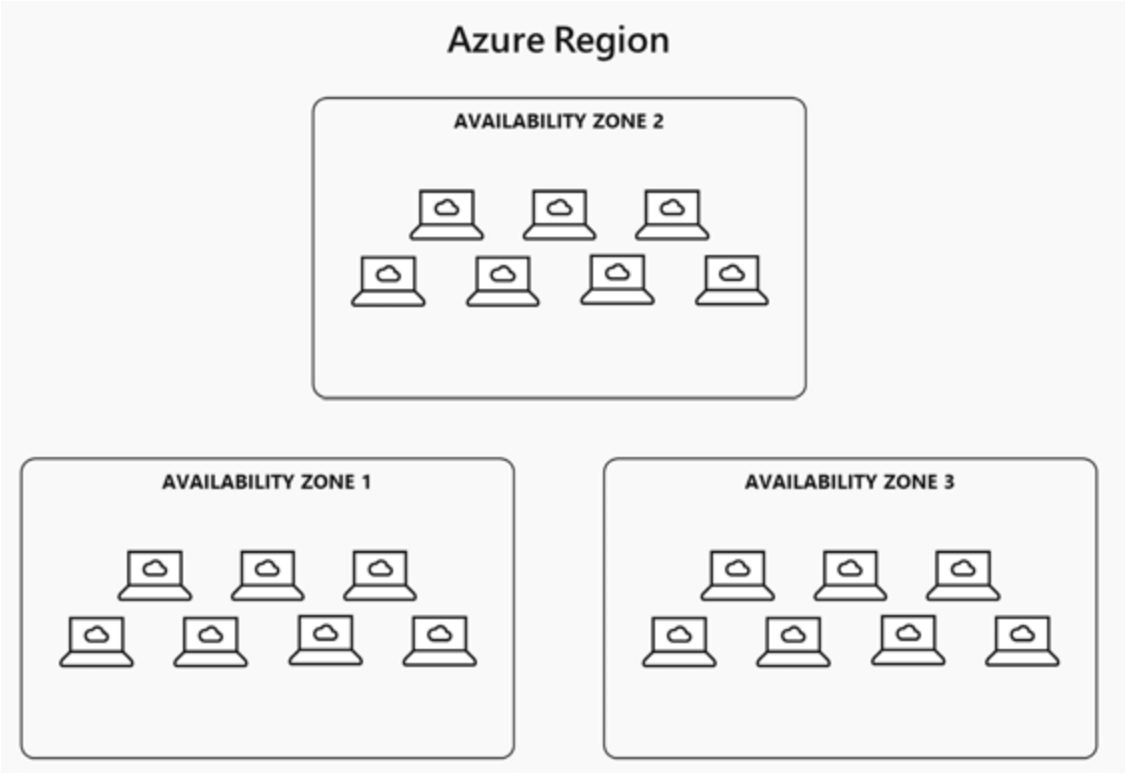


Figure 4.8: Azure Region

Sizes and performance of fixed-price licenses

The way Windows 365 works is a little bit different from how other virtualization services work. The performance of your Cloud PC is defined per user-assigned license via the Microsoft 365 admin center portal in the same manner as how you assign, for example, Microsoft 365 E3/E5 licenses to users.

There are multiple licenses that reflect different VM sizes. Think about more vCPUs, RAM and OS, and profile storage. Graphically enhanced sizes are now supported in public preview!

The following table has all the different Cloud PC licenses that are available today. GPU-enhanced Cloud PC sizes will be added soon, and will most likely already be available when you read this book:

VM/OS disk size	Example scenarios	Applications
2 vCPU/4 GB/256 GB 2 vCPU/4 GB/128 GB 2 vCPU/4 GB/64 GB	Mergers and acquisitions, short-term and seasonal, customer services, BYOPC, work from home	Microsoft 365 Apps, Microsoft Teams (audio-only), Outlook, Excel, PowerPoint, OneDrive, Adobe Reader, Edge, line-of-business app(s), and Defender support
2 vCPU/8 GB/256 GB 2 vCPU/8 GB/128 GB	BYOPC, work from home, market researchers, government, consultants	Microsoft 365 Apps, Microsoft Teams, Outlook, Excel, Access, PowerPoint, OneDrive, Adobe Reader, Edge, line-of-business app(s), and Defender support
4 vCPU/16 GB/512 GB 4 vCPU/16 GB/256 GB 4 vCPU/16 GB/128 GB	Finance, government, consultants, healthcare services, BYOPC, work from home	Microsoft 365 Apps, Microsoft Teams, Outlook, Excel, Access, PowerPoint, Power BI, Dynamics 365, OneDrive, Adobe Reader, Edge, line-of-business app(s), Defender support, nested virtualization support; Windows Subsystem for Linux/Android, Hyper-V, and Defender support
8 vCPU/32 GB/512 GB 8 vCPU/32 GB/256 GB 8 vCPU/32 GB/128 GB	Software developers, engineers, content creators, design and engineering workstations	Microsoft 365 Apps, Microsoft Teams, Outlook, Access, OneDrive, Adobe Reader, Edge, Power BI, Visual Studio Code, line-of-business app(s), nested virtualization support; Windows Subsystem for Linux/Android, Hyper-V, and Defender support
16 vCPU/64 GB/1 TB 16 vCPU/64 GB/512 GB 16 vCPU/64 GB/256 GB 16 vCPU/64 GB/128 GB	Software developers, engineers, content creators, design and engineering workstations	Microsoft 365 Apps, Microsoft Teams, Outlook, Access, OneDrive, Adobe Reader, Edge, Power BI, Visual Studio Code, line-of-business app(s), Nested Virtualization support; Windows Subsystem for Linux/Android, Hyper-V, and Defender support
GPU 4 vCPU, 16 GB RAM, 4 GB vRAM, 512 GB GPU 8 vCPU, 56 GB, 12 GB vRAM, 1TB 16 vCPU, 110 GB, 16 GB vRAM, 1TB	Software developers, engineers, content creators, design and engineering workstations	Adobe Photoshop, Illustrator, AutoCAD, Revit, Solidworks, Microsoft 365 Apps, Microsoft Teams, Outlook, Access, OneDrive, Adobe Reader, Edge, Power BI, Visual Studio Code, line-of-business app(s), nested virtualization support; Windows Subsystem for Linux/Android, Hyper-V, and Defender support

Table 4.2: Cloud PC licenses

Per the license scenario, you will gain a certain level of performance benefit. You can use the following graph as a reference to architect the right set of licenses to achieve the performance your users need.

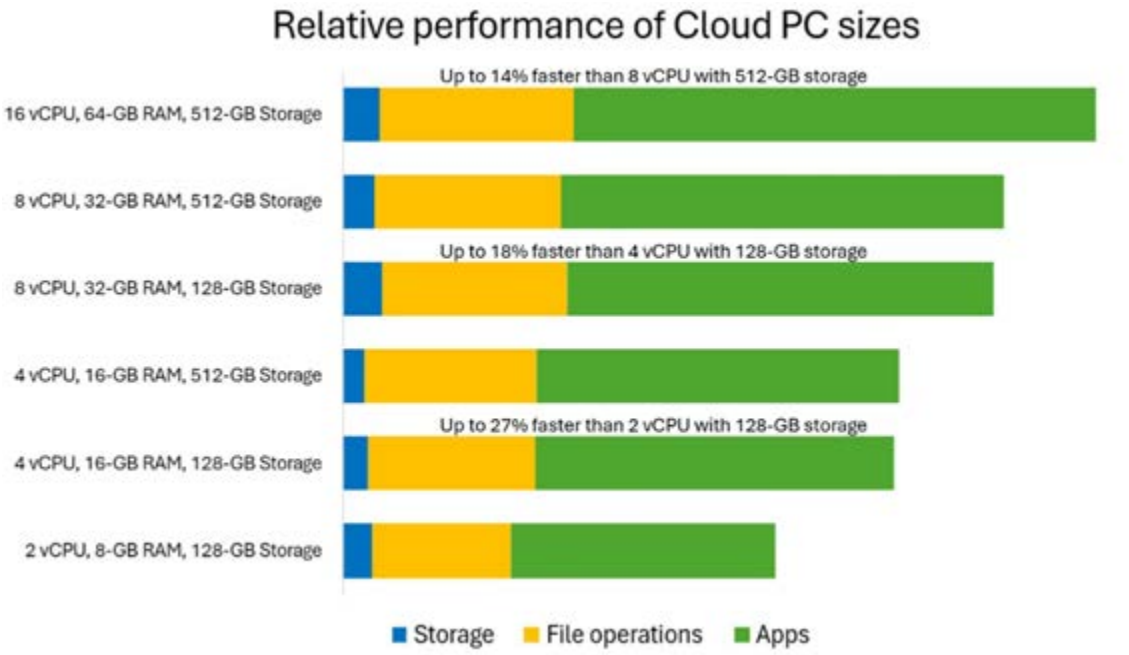


Figure 4.9: Relative performance of Cloud PCs

GPU-Enhanced Cloud PCs

Whether you are a graphic designer, video editor, 3D modeler, data analyst, or visualization specialist, you can now enjoy the GPU acceleration you need to work efficiently on any device and from any location.

With Windows 365, you always have access to the latest hardware in Microsoft Azure, so you don't have to worry about hardware life cycles. Powered by NVIDIA and AMD, GPU-enabled Cloud PCs are designed to handle workloads that involve graphic design, image and video rendering, 3D modeling, data processing, and visualization applications that require a GPU to perform. Example applications include Adobe Photoshop, Illustrator, or enhanced video editing / 3D software. For engineering workloads, AutoCAD, Revit, SolidWorks, and other technical drawing software are supported.

These high-performance offerings are now in public preview in selected regions, and they come in the following configurations:

- Windows 365 Enterprise GPU 4 vCPU, 16 GB RAM, 4 GB vRAM, 512 GB
- Windows 365 Enterprise GPU 8 vCPU, 56 GB, 12 GB vRAM, 1TB
- Windows 365 Enterprise GPU 16 vCPU, 110 GB, 16 GB vRAM, 1TB

With GPU-enhanced Cloud PCs and our recent RDP protocol enhancements, we have been able to deliver over 220 FPS during benchmark tests!

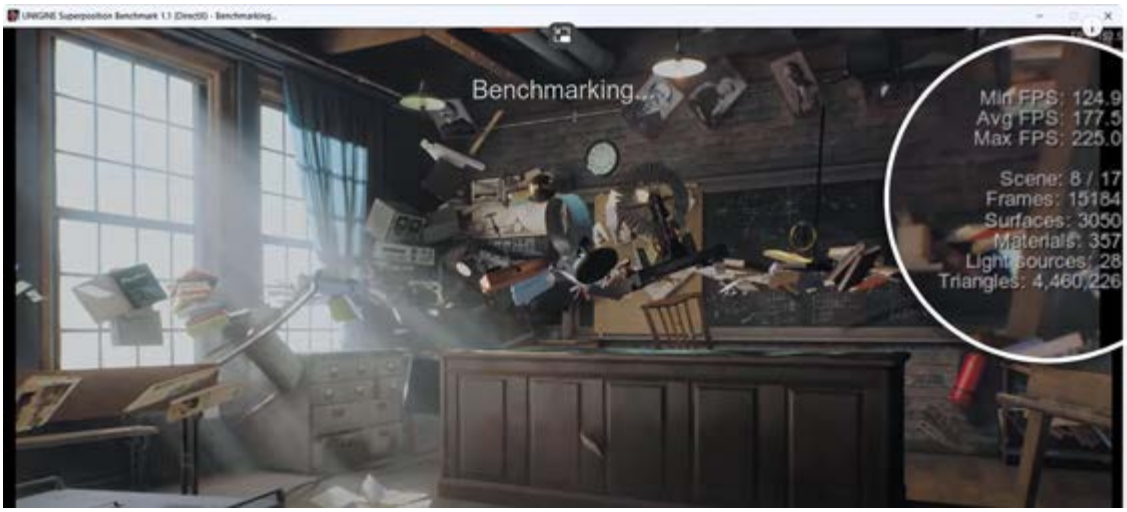


Figure 4.10: Cloud PCs benchmarking

Connect to your on-premises network

Most likely, you will need to connect to backend services with your Cloud PC, which are either living in a private cloud data center on-premises or in Azure. Windows 365 Enterprise supports all Azure networking services to connect to your own networks via ExpressRoute, Site2Site VPN, or SD-WAN. You must configure this via Azure Networking, meaning it requires an Azure subscription, VNet, and VPN connection. For a POC, you can easily configure a site-to-site VPN connection to ensure your Cloud PCs can talk with your intranet, databases, and application servers.

Once you have this ready, you must move to the Intune portal to configure an **Azure Network Connection** (**ANC**) that you need to have first before creating the provisioning policy (covered in the next section). There are two kinds of ANCs based on their join type. Both let you manage traffic and Cloud PC access to network-based resources, but they have different connectivity requirements:

- **Microsoft Entra join**: This doesn't require connectivity to a Windows Server AD domain.
- **Hybrid Microsoft Entra Join**: This requires connectivity to a Windows Server AD domain. You must provide the AD domain details when you create the ANC.

We recommend customers pick the hosted network option for a more streamlined and as-a-service networking model for their Cloud PCs.

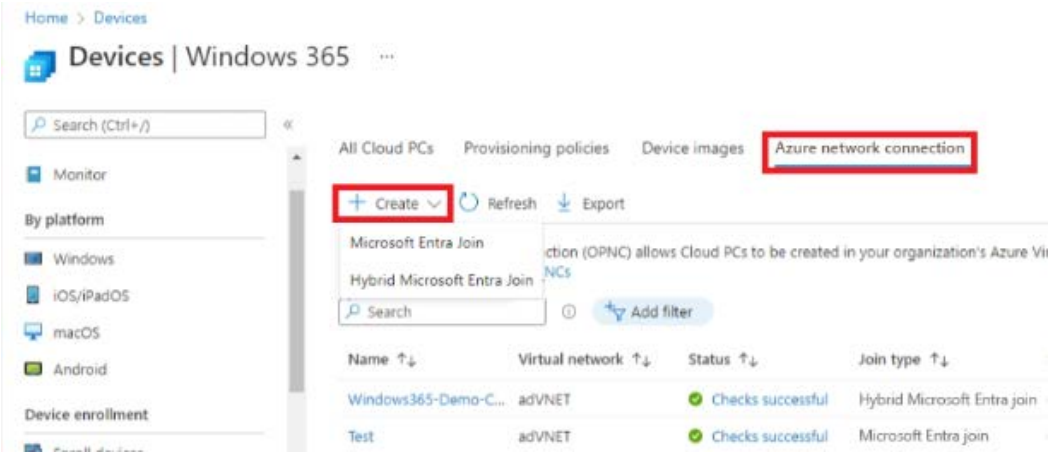


Figure 4.11: Azure network connection

More in-depth information about this and how you can configure it can be found later, in *Chapter 5*, *Deploying Windows 365*.

Provisioning policies

A provisioning policy is what the name suggests – a policy to provision your Cloud PCs. The policy must be configured after you have configured the on-premises connection as this is one of the requirements to move forward.

The provisioning policy includes the baseline configuration of your Cloud PC, such as the image version of Windows 10 Enterprise or Windows 11, the on-premises connection (location), and the Entra ID group that includes the users that should receive this baseline configuration.

Once the provisioning policy is done, it will show up under the **Provisioning policies** menu. You can have multiple policies per department or location as this would be the most common reason for enterprises to split them into different provisioning policies.

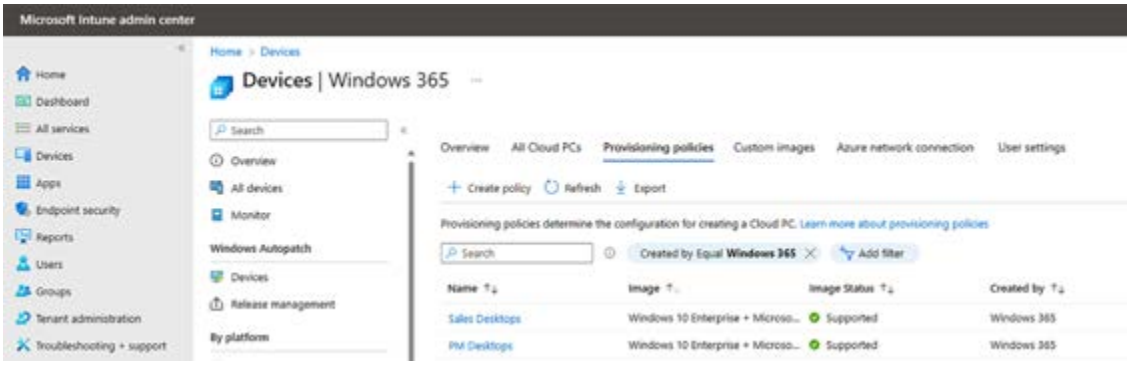


Figure 4.12: Provisioning policies

Now that the information you need to know about provisioning policies has been explained, we will take a deeper dive into the images that are supported as part of the provisioning policy.

Windows 365 – gallery images

As written in the previous section, the image selection option is part of the provisioning policy. There's also the option to select a gallery image running Windows 10 or 11 with pre-baked images per workload type.

It is important to mention that the images with **+ Microsoft 365 Apps** next to them include Office Apps pre-installed on a base Windows 10 or Windows 11 build. The OS optimizations version includes edits to the Windows OS, enhancing its performance to operate more efficiently and be optimized for virtualized Windows.

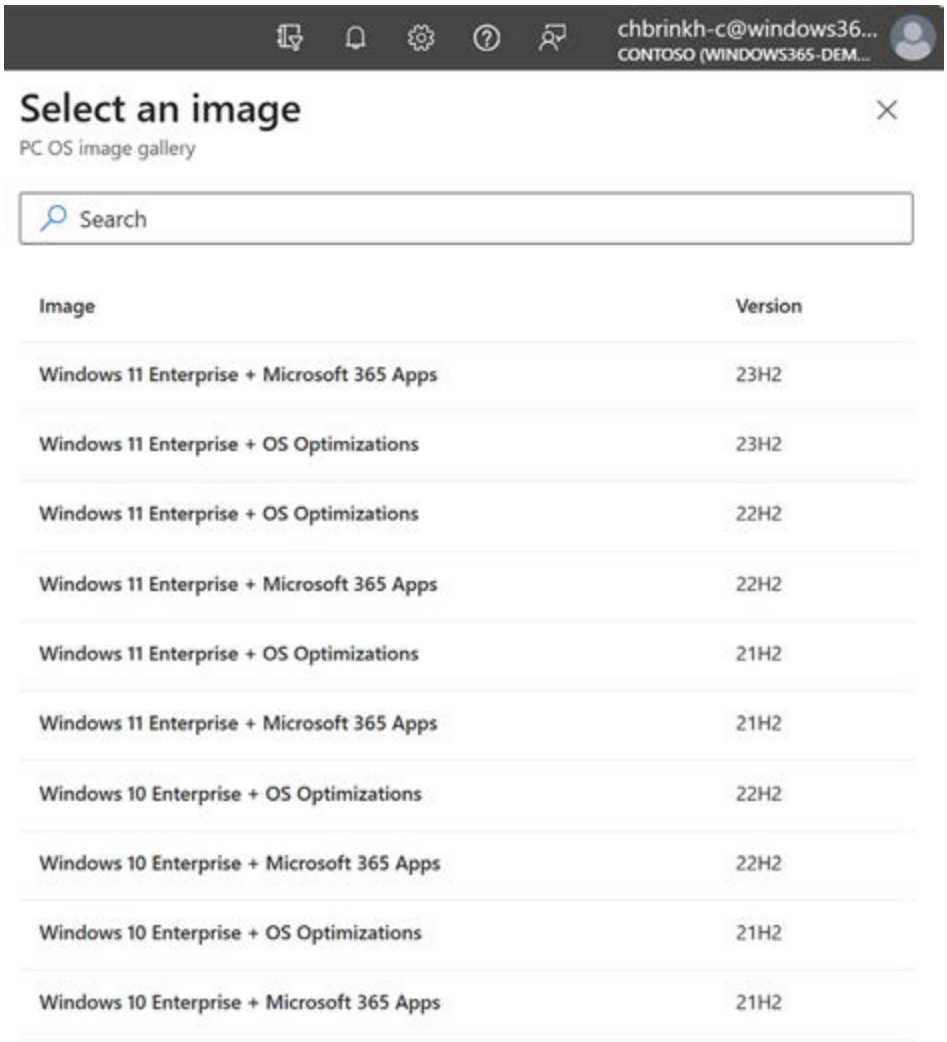


Figure 4.13: Selecting Windows 365 images

Now, we've explained how you could use the preferred route in selecting images for Windows 365 Cloud PCs. In the next section, we explain how you can use custom images.

Custom images

You can use custom images (also referred to as a golden image) if desired. To do so, you need to preload your images via Azure as a **Managed Image** or the **Shared Image Gallery**. To learn more about creating custom images with Windows 365, see `https://learn.microsoft.com/en-us/windows-365/enterprise/add-device-images`.

To get the benefits, like simple and unified management options of modern management, we strongly recommend using the gallery images included in Windows 365 and using Intune to install applications. While in VDI, you may have updated your image on a weekly basis, using a gallery image eliminates the challenge of repeatedly updating your custom image whenever a single component changes. All images will be updated monthly by Microsoft at patch Tuesday. We recommend customers use Windows Autopatch to simplify Windows Updates in conjunction with Windows 365.

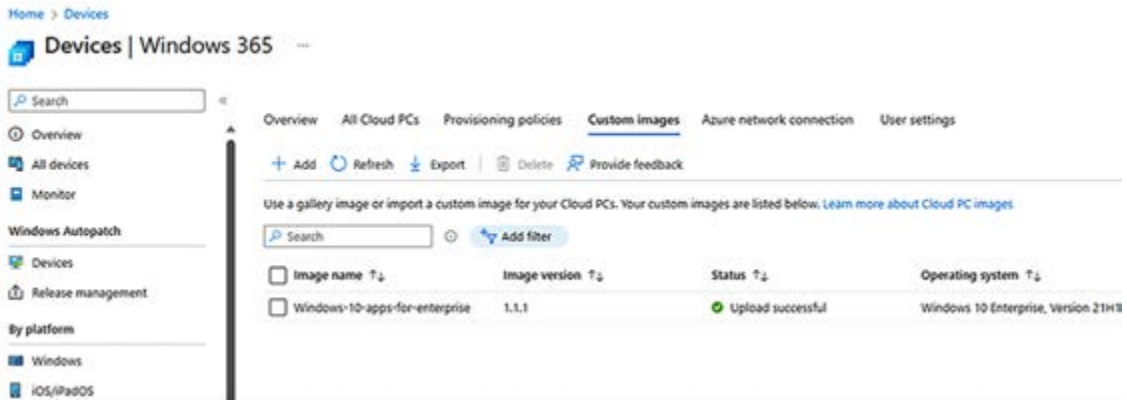


Figure 4.14: Selecting Windows 365 images

Windows Updates via Autopatch

Updating your images is something we recommend doing every patch Tuesday. How nice would it be if you could have Microsoft taking care of your Windows Updates as part of another Microsoft cloud service? That's exactly what Windows Autopatch is. Windows Autopatch helps you minimize the involvement of your scarce IT resources in the planning and deployment of updates for Windows, Microsoft 365 Apps, Microsoft Edge, or Teams.

Windows Autopatch uses careful rollout sequences and communicates with you throughout the release, allowing your IT Admins to focus on other activities and tasks. Learn how to enable Windows Autopatch as a tenant setting in Microsoft Intune in *Chapter 7*.

Enabling Windows Autopatch for Cloud PCs is extremely easy. You simply enable it via the provisioning policy process and you're all set. See how to create a provisioning policy in Windows 365 in the following figure.

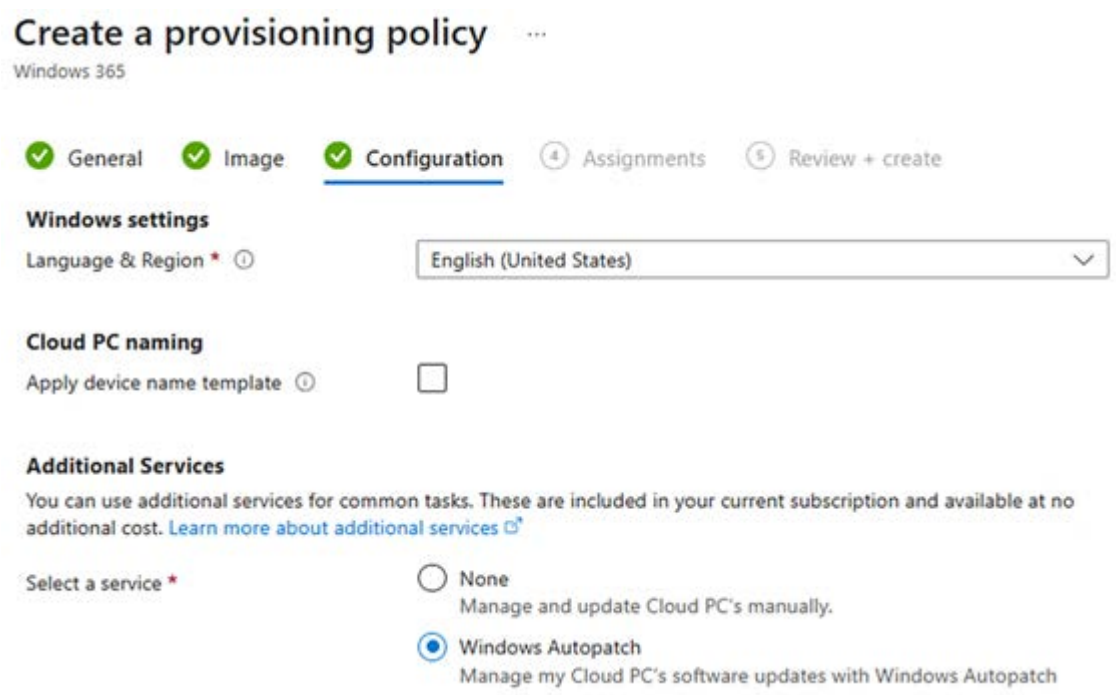


Figure 4.15: Windows Autopatch

Roles and delegation

Windows 365 offers capabilities to delegate access features and functionalities on top of existing Intune roles within Microsoft Intune; for example, you want to give helpdesk employees read-only access to the Windows 365 portal to check whether the Cloud PC is unavailable or not. Other examples include the separation of security-related settings as part of your security policies. Let us explain all the roles in more depth in the following table:

Role	In	Can do
Application Manager	Windows 365 Enterprise Cloud PC	Intune Application Managers can manage applications, read device information, and view device configuration profiles.
Cloud PC Administrator	Windows 365 Enterprise Cloud PC	Cloud PC Administrators can take read and write actions in the Cloud PC L2 node in MEM.
Cloud PC Reader	Windows 365 Enterprise Cloud PC	Cloud PC Readers can lake read actions in the Cloud PC L2 node in MEM.

Endpoint Security Manager	Windows 365 Enterprise Cloud PC	Intune Endpoint Security Managers can manage security and compliance features such as security baselines, device compliance, Conditional Access, and Microsoft Defender for Endpoint for their Cloud PCs.
Help Desk Operator	Windows 365 Enterprise Cloud PC	Intune Help Desk Operators can perform remote tasks on Cloud PCs and assign applications or policies to the devices.
Intune Role Administrator	Windows 365 Enterprise Cloud PC	Intune administrator role can assign Intune roles (built-in and custom) to other administrators but cannot assign Cloud PC roles.
Policy and Profile Manager	Windows 365 Enterprise Cloud PC	Intune Policy and Profile Managers can manage compliance policy, configuration profiles, corporate device identifiers, and security baselines for Cloud PCs.
Read Only Operator	Windows 365 Enterprise Cloud PC	Intune Read Only Operators have read-only access to all Intune nodes including the Cloud PC node.
School Administrator	Windows 365 Enterprise Cloud PC	Intune School Administrators can manage Windows 10 devices in Intune for Education.

Table 4.3: Roles and delegation

In the following screenshot, see the list of roles available in the Microsoft Intune admin center portal:

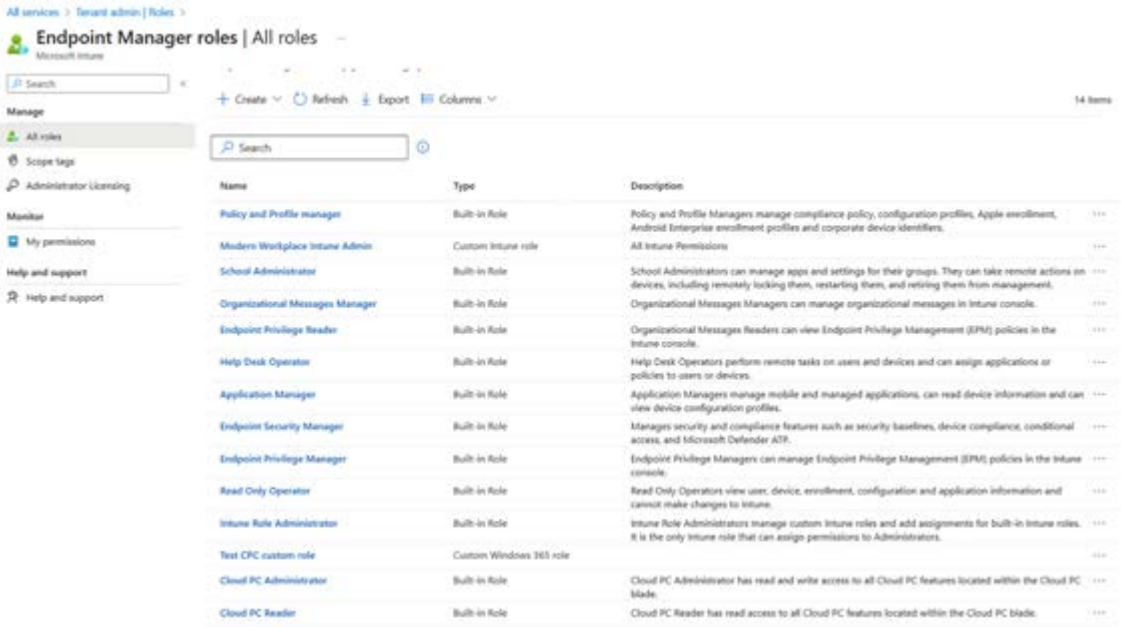


Figure 4.16: Available Cloud PC roles in Microsoft Intune

Assign them directly to your users or Entra ID groups to make them more dynamically available.

The Watchdog service

Earlier in this chapter we shared the vision of Windows 365, making the management and maintenance much easier to use as a replacement for complex VDI-related infrastructure where you have to maintain multiple different tools via separate interfaces. The Watchdog service can be compared to a canary in a coal mine, alerting miners to hidden danger, and is a great example of taking care of work that you normally must troubleshoot yourself.

After you have finished with the configuration of the on-premises network connection (explained later in this chapter in more detail), the Watchdog service will check your environment for all the prerequisites to use Windows 365, so you need to think about the following items:

- Checking on service URLs
- Network access
- DNS resolving
- Rights to create computer accounts in the right organizational unit
- Entra ID Connect configuration
- Subnet range – are there enough IP addresses available for your deployment?
- Endpoint connectivity (Intune and AV service URLs)

The other great thing about the Watchdog service is that it constantly runs in the background. For example, if something changes in your environment, it will try to fix it for you – or send you, the IT admin, a notification with the resolution of the problem!

In the following screenshots, you can find the result of a successful Watchdog check. You see that it outlines all the requirements for a successful Windows 365 deployment, and more:

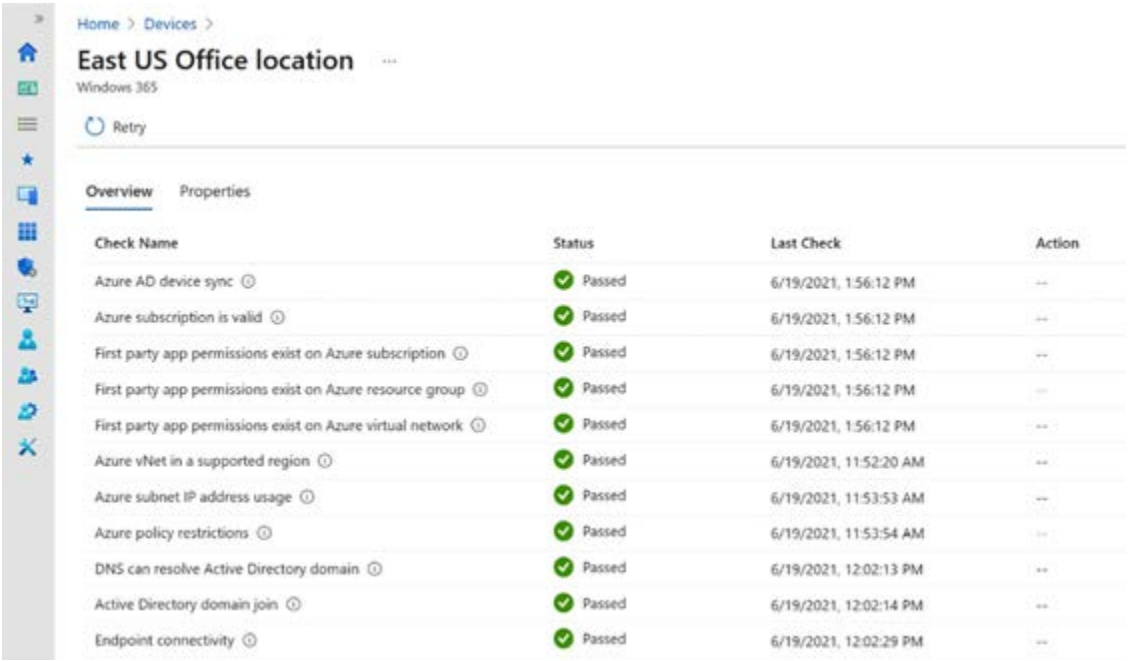


Figure 4.17: Watchdog service – Hybrid Entra ID checks

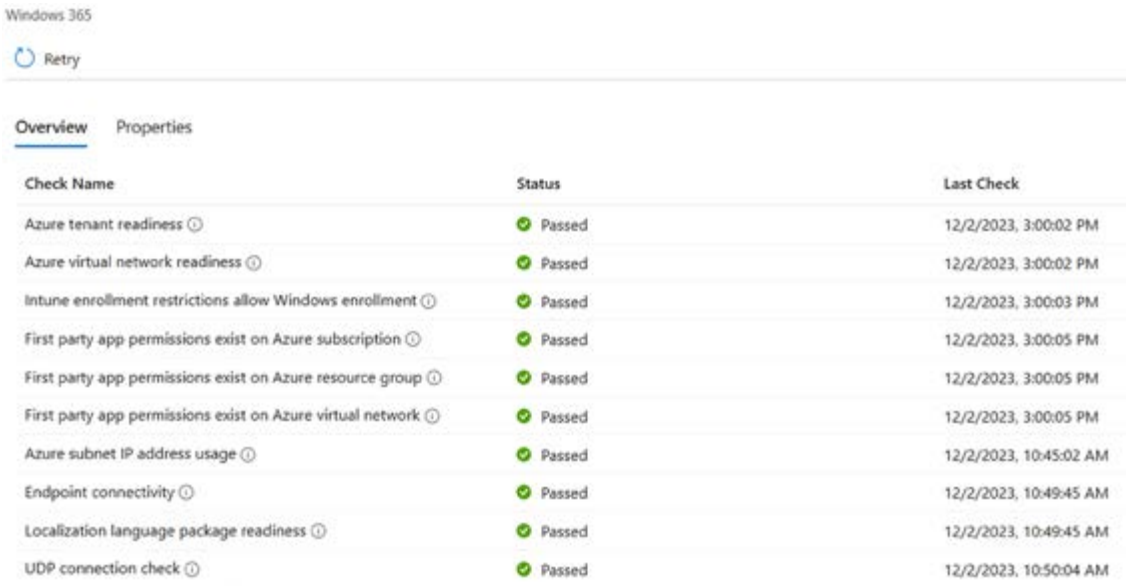


Figure 4.18: Watchdog service – Entra ID Join checks

Optimized Teams on Windows 365

The Windows images provided by Microsoft in the gallery as part of the provisioning policy configuration process include all the software that is needed to offer an optimized Teams experience as part of your Cloud PC. As an IT admin or user, you only need to install and configure the Microsoft Teams application and then you are ready to use it.

The main benefit of this approach is that you set up Teams audio and video calls directly, peer to peer, from your physical endpoint to the other person, which effectively creates the same experience as you would have on a physical endpoint running Microsoft Teams.

Some of the key benefits of the optimizations are the following:

- High-performance peer-to-peer streaming – traffic will flow peer-to-peer and be rendered via the endpoint.
- Devices will be redirected as the same hardware device, providing better hardware redirection support.
- On Windows and MacOS clients, all the benefits of the modern media stack, including hardware video decoding.

Screen capture protection and watermarking

The screen capture protection feature prevents sensitive information from being captured on the client endpoints. When you enable this feature, remote content will be automatically blocked or hidden in screenshots and screen shares.

It will also be hidden from malicious software that may be continuously capturing your screen's content. We recommend you disable clipboard redirection to prevent the copying of remote content to endpoints while using this feature.

To enable the screen capture protection feature, you only have to enable it via the new AVD – CSP policies in the settings catalog.

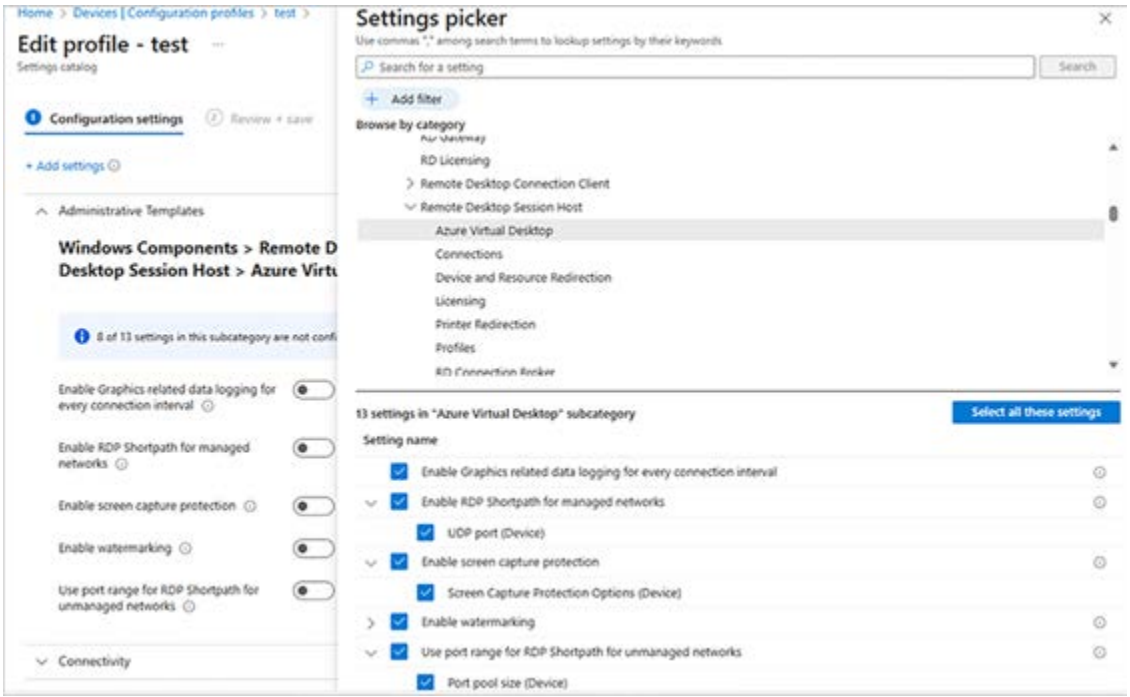


Figure 4.19: Screen capture protection and watermarking

Migrate GPOs to a Settings Catalog policy

Want to migrate your existing AD-based Group Policies into Microsoft Intune? This can be done with Group Policy analytics. Import your on-premises GPOs and create an Intune policy using your imported settings that can then be deployed to users and devices managed by your organization.

Based on the import and current usage, Group Policy analytics can find the equivalent setting in the settings catalog, which you can read more about in *Chapter 9*:

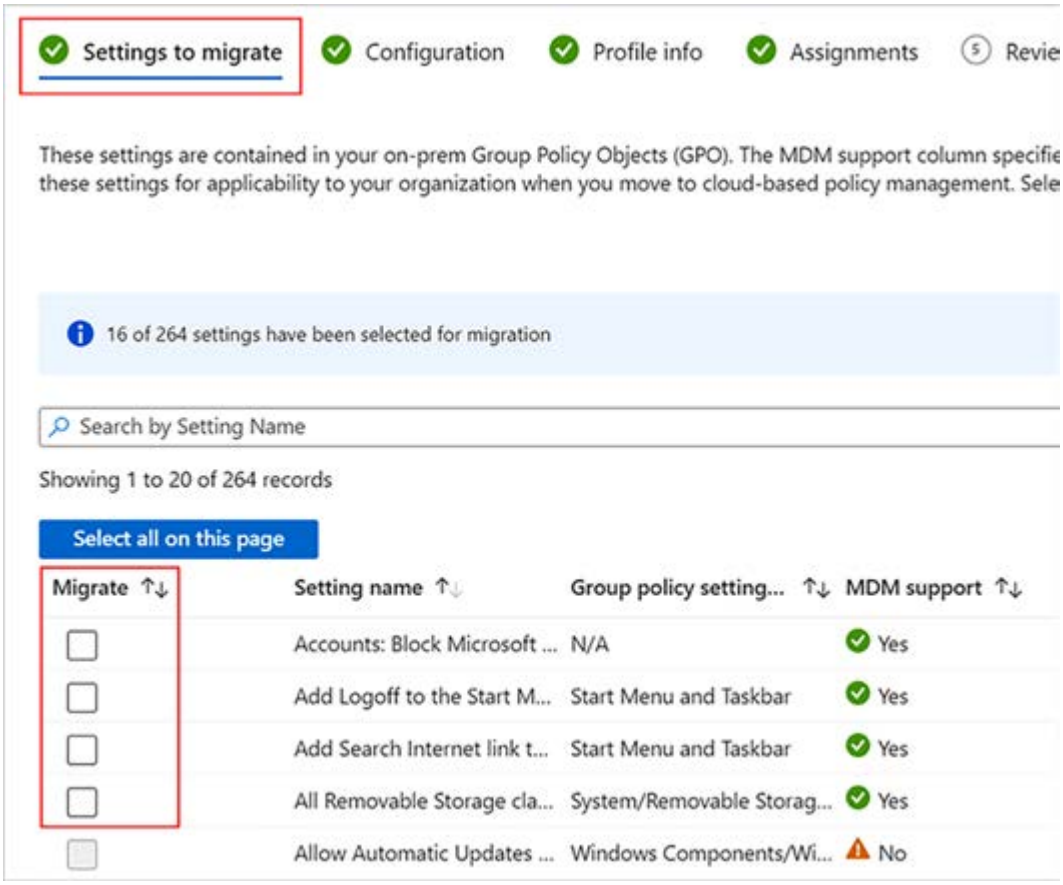


Figure 4.20: Group Policy analytics

Summary

In this chapter, you've learned everything about the fundamentals of the new Windows 365 service. *Are you ready to learn how to kick the tires!?*

In the next chapter, we will learn how to deploy Windows 365.

Questions

1. What cloud-managed service is used to manage, maintain, and operate your Windows 365 cloud desktops?

    a. Microsoft Intune
    b. Microsoft Endpoint Configuration Manager
    c. System Center Configuration Manager

2. Do Cloud PCs running inside a Microsoft-managed environment configured with Entra ID Join Cloud PCs in a hosted network mean that you don't need an Azure subscription?

    a. Yes
    b. No

Answers

1. (a)
2. (a)

Further reading

If you want to learn more about Windows 365 after reading this section, please go to one of the following chapters of this book:

- *Chapter 5*, *Deploying Windows 365*
- *Chapter 14*, *Monitoring and Endpoint Analytics*
- *Chapter 17*, *Troubleshooting Windows 365*

Join the CloudPro Newsletter with 44000+ Subscribers

Want to know what's happening in cloud computing, DevOps, IT administration, networking, and more? Scan the QR code to subscribe to **CloudPro**, our weekly newsletter for 44,000+ tech professionals who want to stay informed and ahead of the curve.



https://packt.link/cloudpro

5

Deploying Windows 365

In this chapter, you'll learn everything you need to know about how to deploy Windows 365, such as what the requirements are, how to connect to Cloud PCs via the new Windows App, Windows 365 Boot and Switch, and other tips and tricks to configure Cloud PCs in the most secure way possible.

After this chapter, you'll know everything you need to get started with this Windows 365 cloud service, which simplifies deployment as well as Cloud PC maintenance with Microsoft Intune.

This chapter is very comprehensive and covers the following topics:

- Technical requirements for deploying Windows 365
- Required URLs
- **Remote Desktop Protocol** (**RDP**) requirements
- Connect to on-premises networks (optional)
- Learn how to provision a Cloud PC
- Custom image management
- Moving Cloud PCs
- Security baselines
- Restore points
- Connecting to your Cloud PC
- Windows App
- User Actions
- Supported redirections per platform
- Windows 365 Boot shared mode
- Windows 365 Boot dedicated mode
- Windows 365 Switch
- Monitoring and analytics
- Windows 365 AI
- Windows 365 and Intune Suite

- Enterprise app management
- Remote Help

Technical requirements for deploying Windows 365

To use Windows 365, you must meet the following requirements. For Entra ID Join, you do not need to bring in an Azure subscription or Azure vNet.

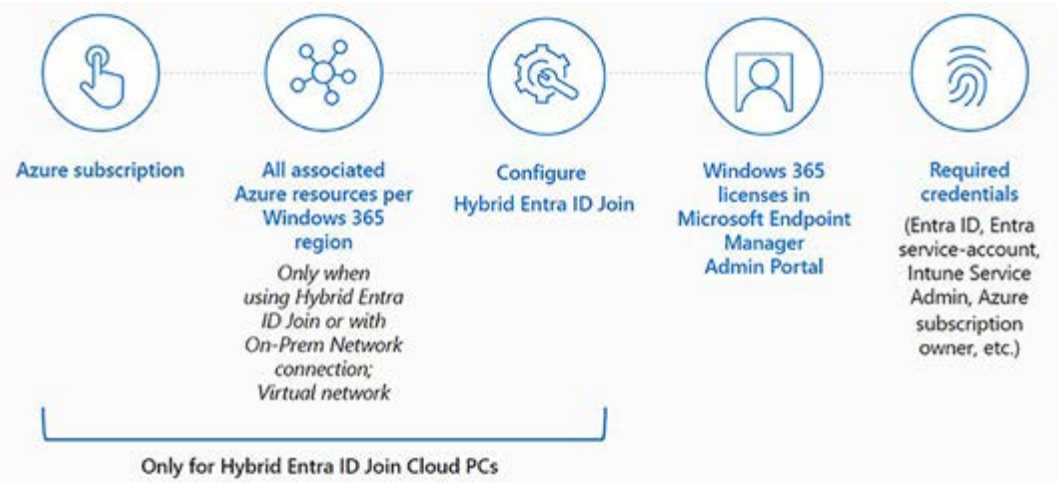


Figure 5.1: Technical requirements for deploying Windows 365

Required URLs

For the connection to be established, certain URLs must be allowed on the client network that the user is connected to and, likewise, the network the Cloud PC is connected to must allow specific outbound URLs. Be aware there are different URLs for the Azure public cloud and Azure Cloud for US Government; see the following tables to find the URL requirements.

The Azure **Virtual Network(s)** (**VNets**) you create for Windows 365 is required to have outbound TCP access to the underlying services we use as part of the firewall rules in the customer's Azure subscription.

In the following tables, you will find a snippet of what URLs and ports are required to open to communicate with the Windows 365 service.

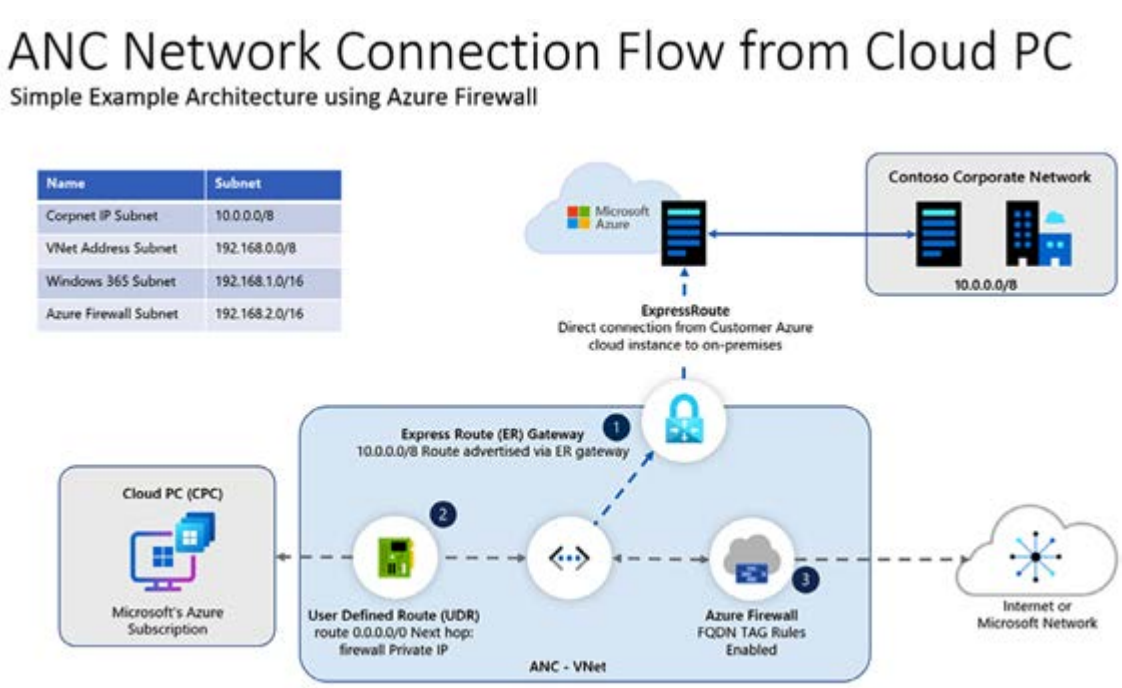


Figure 5.2: ANC Network Connection Flow from Cloud PC

Find the full list of all the required Windows 365 URLs at `https://aka.ms/W365URLs`.

Find the full list of all the required Microsoft Intune URLs at `https://aka.ms/MEMURLs`.

URL	Outbound TCP Port	Purpose
`login.microsoftonline.com`	443	Microsoft Online Services authentication
`*.wvd.microsoft.com`	443	Service traffic
`*.servicebus.windows.net`	443	Troubleshooting data
`go.microsoft.com`	443	Microsoft FWLinks
`aka.ms`	443	URL shortener
`learn.microsoft.com`	443	Documentation
`privacy.microsoft.com`	443	Privacy statement
`query.prod.cms.rt.microsoft.com`	443	Client updates (only Windows clients)

Table 5.1: Client network URL requirements in Azure public cloud

URL	Outbound TCP Port	Purpose
login.microsoftonline.us	443	Microsoft Online Services authentication
*.wvd.azure.us	443	Service traffic
*.servicebus.usgovcloudapi.net	443	Troubleshooting data
go.microsoft.com	443	Microsoft FWLinks
aka.ms	443	URL shortener
learn.microsoft.com	443	Documentation
privacy.microsoft.com	443	Privacy statement
query.prod.cms.rt.microsoft.com	443	Client updates (only Windows clients)

Table 5.2: Client network URL requirements in Azure Cloud for US Government

URL	Outbound TCP Port	Purpose
login.microsoftonline.com	443	Microsoft Online Services authentication
*.wvd.microsoft.com	443	Service traffic
*.prod.warm.ingest.monitor.core.windows.net	443	Agent traffic (Azure Monitor)
gcs.prod.monitoring.core.windows.net	443	Agent traffic (Azure Cloud)
catalogartifact.azureedge.net	443	Azure Marketplace
kms.core.windows.net	1688	Windows activation
azkms.core.windows.net	1688	Windows activation
mrsglobalsteus2prod.blob.core.windows.net	443	Agent and SXS stack updates
wvdportalstorageblob.blob.core.windows.net	443	Azure portal support
169.254.169.254	80	Azure instance metadata service endpoint
168.63.129.16	80	Cloud PC health monitoring
oneocsp.microsoft.com	80	Certificates
http://www.microsoft.com	80	Certificates

Table 5.3: Cloud PC network URL requirements in Azure public cloud

URL	Outbound TCP Port	Purpose
login.microsoftonline.us	443	Microsoft Online Services authentication
*.wvd.azure.us	443	Service traffic
*.prod.warm.ingest.monitor.core.usgovcloudapi.net	443	Agent traffic (Azure Monitor)
gcs.monitoring.core.usgovcloudapi.net	443	Agent traffic (Azure Cloud)
kms.core.usgovcloudapi.net	1688	Windows activation
mrsglobalstugviffx.blob.core.usgovcloudapi.net	443	Agent and SXS stack updates
wvdportalstorageblob.blob.core.usgovcloudapi.net	443	Azure portal support
169.254.169.254	80	Azure instance metadata service endpoint
168.63.129.16	80	Cloud PC health monitoring
ocsp.msocsp.com	80	Certificates

Table 5.4: Cloud PC network URL requirements in Azure Cloud for US Government

If you are using Azure Firewall, make sure to use the **Windows365** FQDN tag to make it easier for you to configure Windows 365 URLs. More information can be found at `https://learn.microsoft.com/en-us/azure/firewall/fqdn-tags`.

RDP requirements and optimizations

Over the last 10 years, the RDP has made significant improvements that are making the protocol one of the leading protocols in the industry. For example, RDP Shortpath introduced UDP support frame rates and the latency of sessions is better than ever before for long-distance connections.

Windows 365 uses the **RDP**, so you should follow the same network bandwidth requirements needed for each scenario in your organization.

Please use the following table as guidance while designing your network infrastructure environment for Windows 365:

Scenario	Default mode	H.264/ AVC 444 mode	Description
Idle	0.3 Kbps	0.3 Kbps	The user has paused their work and there are no active screen updates.
Microsoft Word	100-150 Kbps	200-300 Kbps	The user is actively working with Microsoft Word: typing, pasting graphics, and switching between documents.
Microsoft Excel	150-200 Kbps	400-500 Kbps	The user is actively working with Microsoft Excel: multiple cells with formulas and charts are updated simultaneously.
Microsoft PowerPoint	4-4.5 Mbps	1.6-1.8 Mbps	The user is actively working with Microsoft PowerPoint: typing, pasting, modifying rich graphics, and using slide transition effects.
Web browsing	6-6.5 Mbps	0.9-1 Mbps	The user is actively working with a graphically rich website that contains multiple static and animated images. The user scrolls the pages both horizontally and vertically.
Image gallery	3.3-3.6 Mbps	0.7-0.8 Mbps	The user is actively working with the image gallery application: browsing, zooming, resizing, and rotating images.
A video playback	8.5-9.5 Mbps	2.5-2.8 Mbps	The user is watching a 30 FPS video that consumes half of the screen.
Fullscreen video playback	7.5-8.5 Mbps	2.5-3.1 Mbps	The user is watching a 30 FPS video that's maximized to full screen.

Table 5.5: Designing your network infrastructure environment for Windows 365

Connect to on-premises networks (optional)

In the previous chapter, we explained that it's possible to connect from your Cloud PCs to your own data center location. This section explains the technical steps to configure this.

As a result of this configuration, the vNIC network adapter in the Cloud PC will be added to the Azure VNet in your own Azure subscription.

If you do not need to connect to on-premises resources, you won't have to perform the outlined steps. Cloud PCs can be configured with Entra ID Join within the provisioning policy setup to live in the Cloud without any need for on-premises connectivity. This is called the Hosted Network option and is possible to select during the provisioning policy process.

Note: Before you start the following steps, we expect that you have already created an Azure VNet and either site-to-site VPN or ExpressRoute. This normally happens via the Azure Infrastructure or Networking team. Learn more about it via `https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal`.

1. Go into the **Intune admin center** portal and then into Windows 365 under **Devices | Provisioning**.
2. Click on **Azure network connection**.
3. Click on **+ Create**.

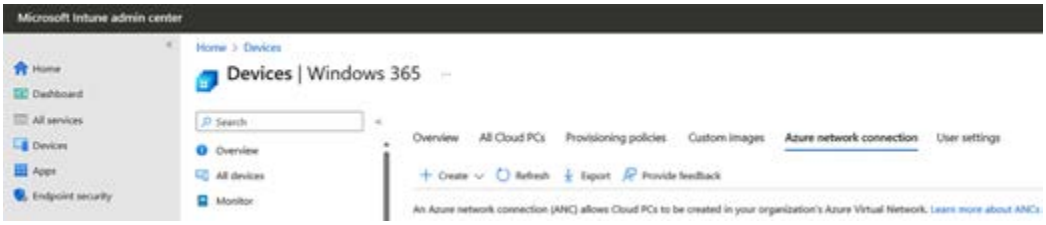


Figure 5.3: Azure network connection

4. Choose whether you want to configure an on-premises connection with **Microsoft Entra ID Join** or **Hybrid Entra ID Join**.

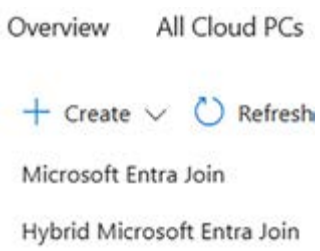


Figure 5.4: Device join type

Entra ID Join

Enter the required technical information regarding your Azure VNet that is configured to connect to your on-premises backend.

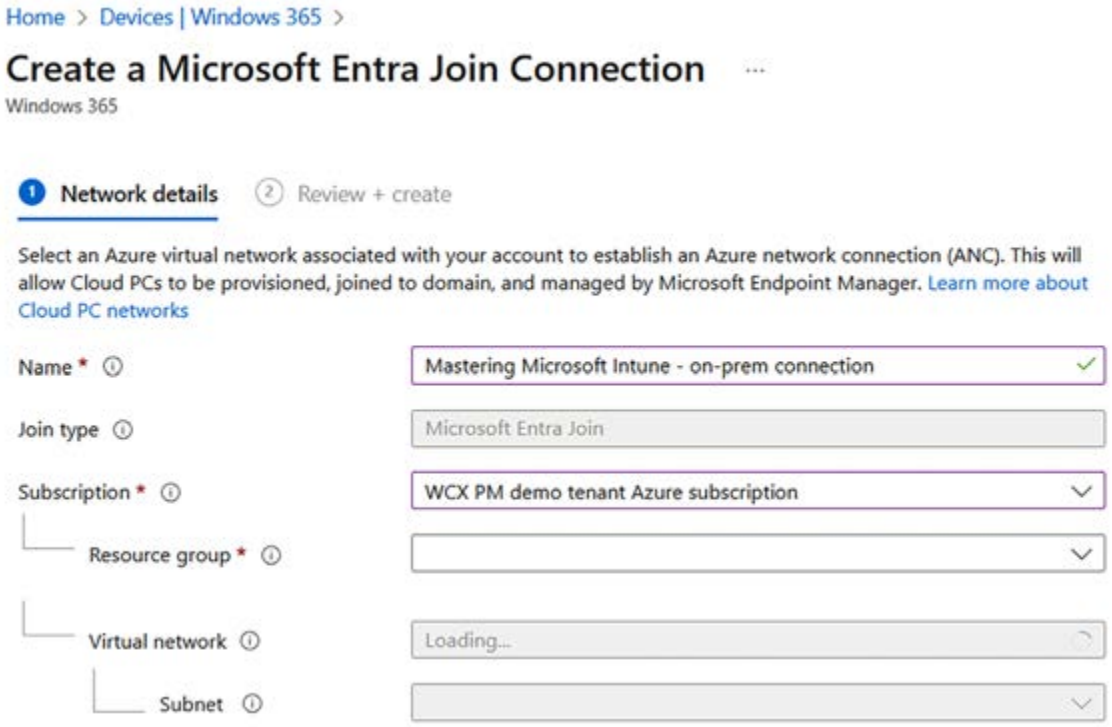


Figure 5.5: Create a Microsoft Entra Join Connection

Hybrid Entra ID Join

Hybrid Entra ID as a provisioning policy option requires more information during the setup to connect to your domain controllers, for example, due to the need for Kerberos, an AD service account is needed as well as an **Organizational Unit** (**OU**).

Also, make sure that your DNS domain name is configured correctly and that it is possible to resolve the domain via your Azure VNet settings – the DNS server that you define as primary.

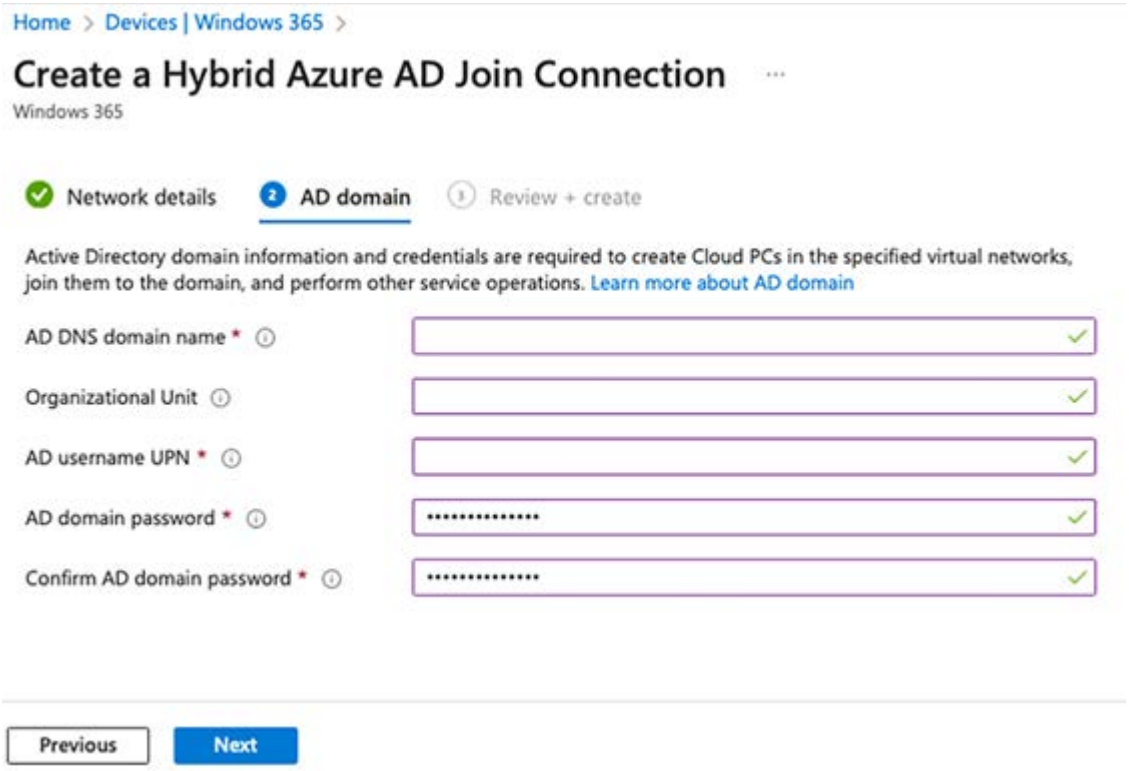


Figure 5.6: Create a Hybrid Azure AD Join Connection

To ensure that the DNS record is working correctly, ensure that your Azure VNet DNS servers point to your own custom DNS servers in order to resolve your internal Kerberos domain name!

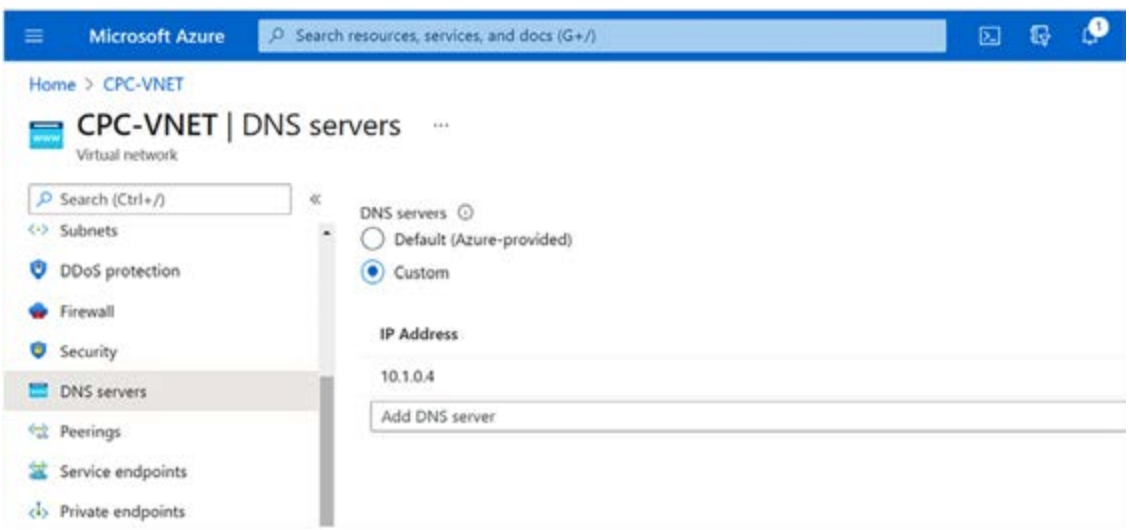


Figure 5.7: Change the DNS servers to custom

Let's start the provisioning of the actual Cloud PCs now!

Purchasing and assigning Cloud PC licenses

Make sure that you have either a trial or production license with Microsoft Intune assigned to your tenant before moving on. Perform the following steps:

1. Go to Microsoft admin center (`https://admin.microsoft.com/`) and purchase a Windows 365 license per size, just like you would with a physical PC.
2. Request a trial via this page: `https://info.microsoft.com/ww-landing-Windows-365-Contact-Me.html?culture=en-us&country=US`.
3. Go to Active users.
4. Open the required user(s).
5. Assign the Windows 365 Cloud PC size license.
6. The following screenshot shows how we assigned a Windows 365 Cloud PC license to Mason, an avid Windows user already:

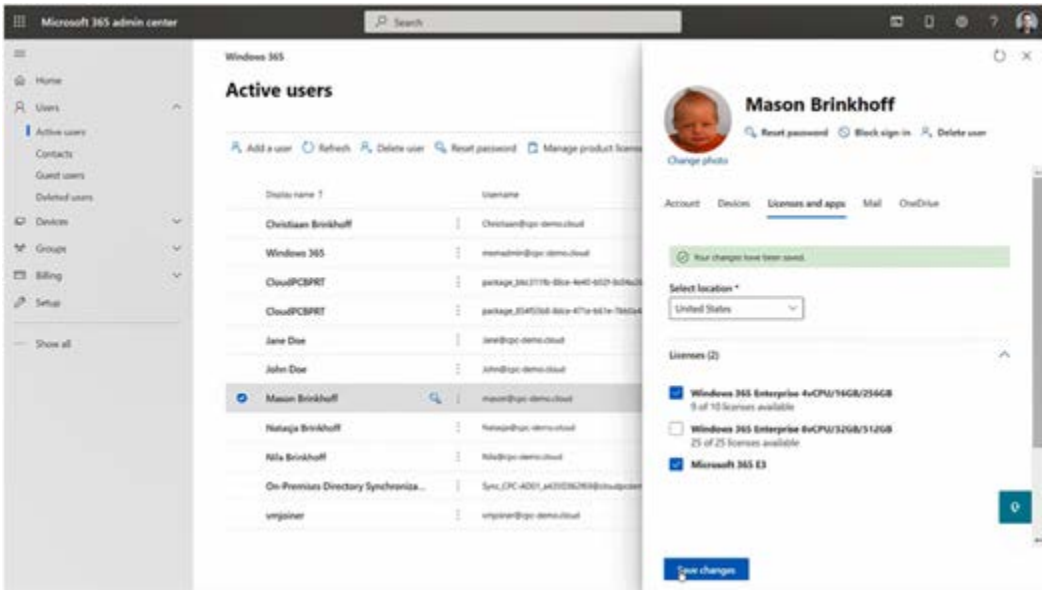


Figure 5.8: Assigning a license

Make sure that the Entra ID/AAD user's location has been set in **Entra ID** before moving on because the location of the user is required to detect the nearest location for the user's backend services.

You can also perform this from the Azure portal or automatically via **Entra ID** group assignment if you're working with more bulk/Enterprise users.

Provision a Cloud PC

In this section, we will be explaining the steps to start the provisioning of one or thousands of Cloud PCs for your business. The steps are extremely simple. Let's go:

1. Open the Microsoft Intune admin portal via intune.microsoft.com.
2. Go to **Devices** | **Provisioning** | **Windows 365**.
3. Go to **Provisioning Policies**.

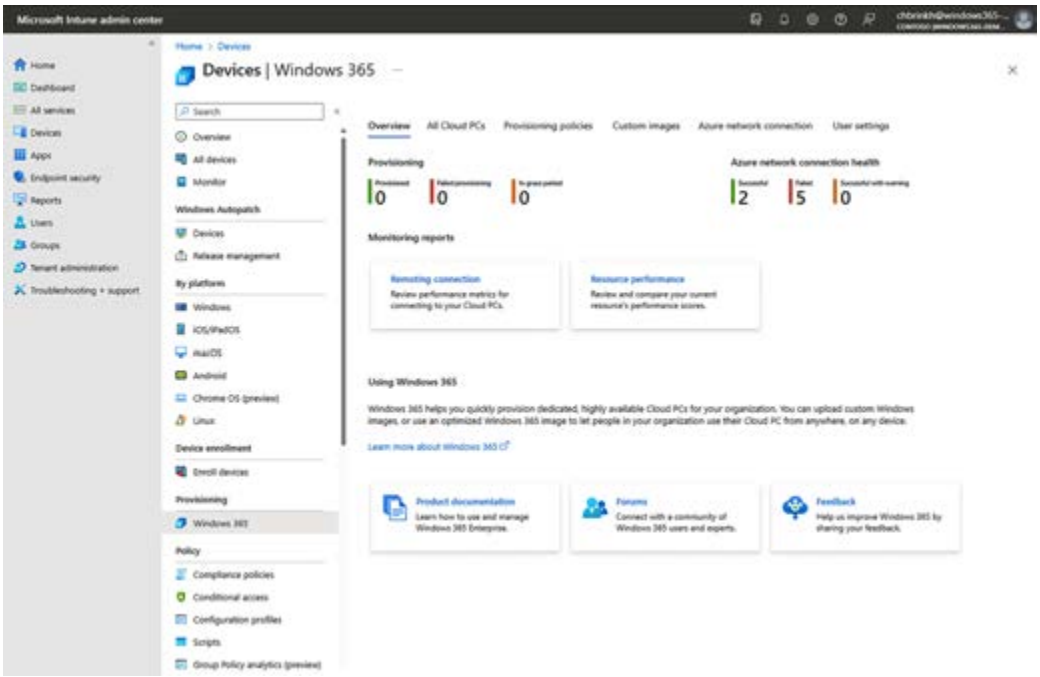


Figure 5.9: Windows 365

4. Click on Create Policy.

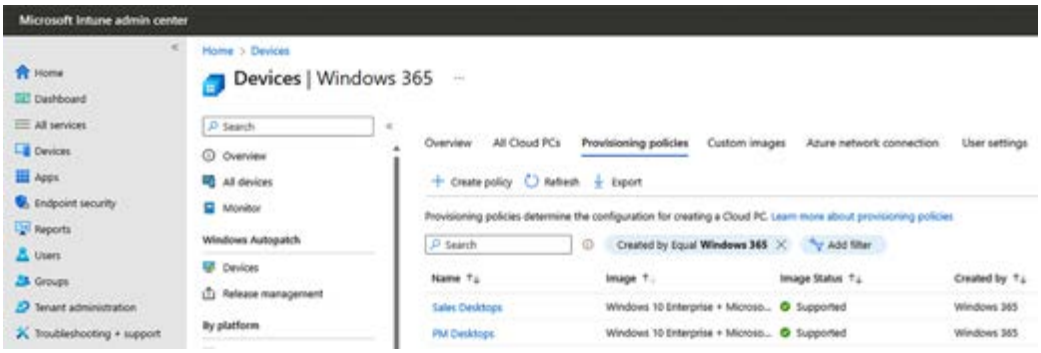


Figure 5.10: Provisioning policies

5. Enter the name of the Provisioning Policy in the **Name** box.

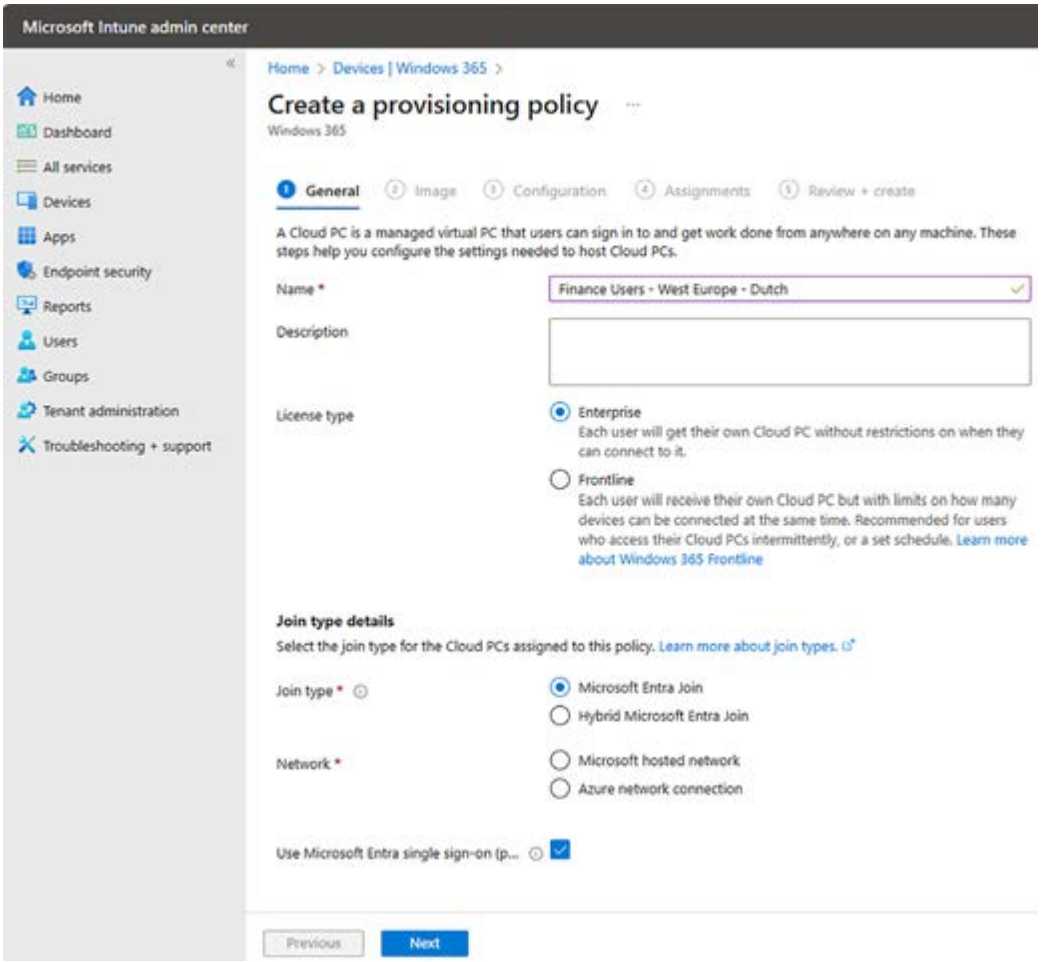


Figure 5.11: Create a provisioning policy

6. Once done, configure your preferred **Join type.** Either Microsoft Entra Join or Hybrid Microsoft Entra Join.
7. Select the **Geography** and **Region** you want to use to deploy your Cloud PCs in. Windows 365 is Multi-Geo and is designed to meet your data residency requirements while retaining single-tenant administration and full-fidelity collaboration experiences between users as necessary.

8. Select whether you want to enable **Single Sign On** (**SSO**) as an end user client experience.

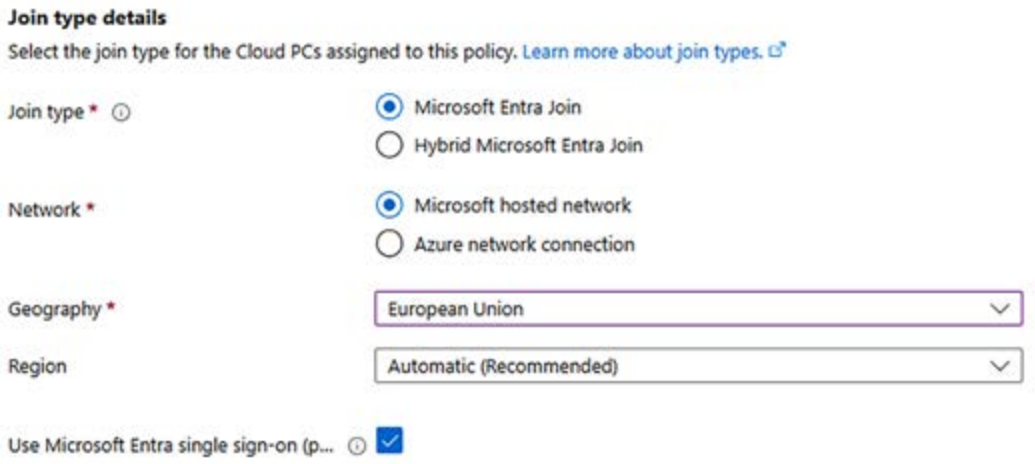


Figure 5.12: Join type details

Note: If you want to connect to your own on-premises network or other Public Cloud or Private Cloud data centers, make sure to select the Azure network connection via the other option during the provisioning policy configuration.

9. With the **Automatic Region** option, you assure yourself of a region that is always available as a fallback. You can also point to one specific region only.
10. If you prefer on-premises network connectivity, you must select Azure network connection. There's a setup process to perform first before you can complete this step. You can find that in the Microsoft docs: `https://learn.microsoft.com/en-us/windows-365/enterprise/create-azure-network-connection`.



Figure 5.13: Network

11. Select the Windows image version you would like to use. We recommend customers use our pre-configured Windows images (known as Gallery images) with Microsoft 365 Apps, Microsoft Teams, Outlook and Edge optimizations, multimedia redirection, and other pre-installed settings like:

    - Services optimized for virtualization
    - UWP packages removed
    - Task scheduler actions disabled

Note: You are also able to use custom images as a selectable option. Make sure to first upload your images via Azure as a Managed Image or via the Shared Image Gallery. We explain these steps later in this chapter.

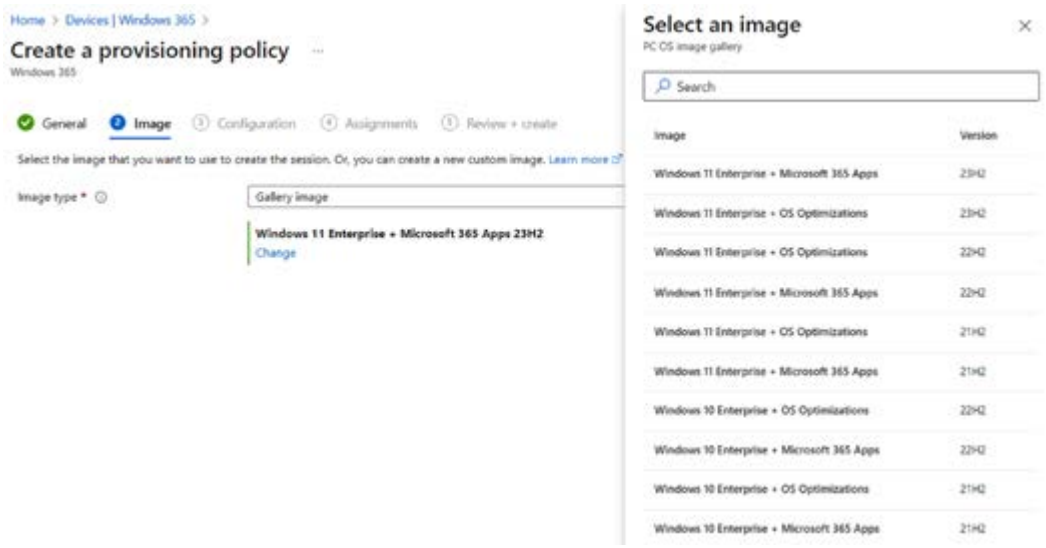


Figure 5.14: Select an image

12. Now, select the language and region for the targeted Cloud PC users.

    For example, if you want your Dutch users to get a Dutch operating system, select **Dutch (Netherlands).**

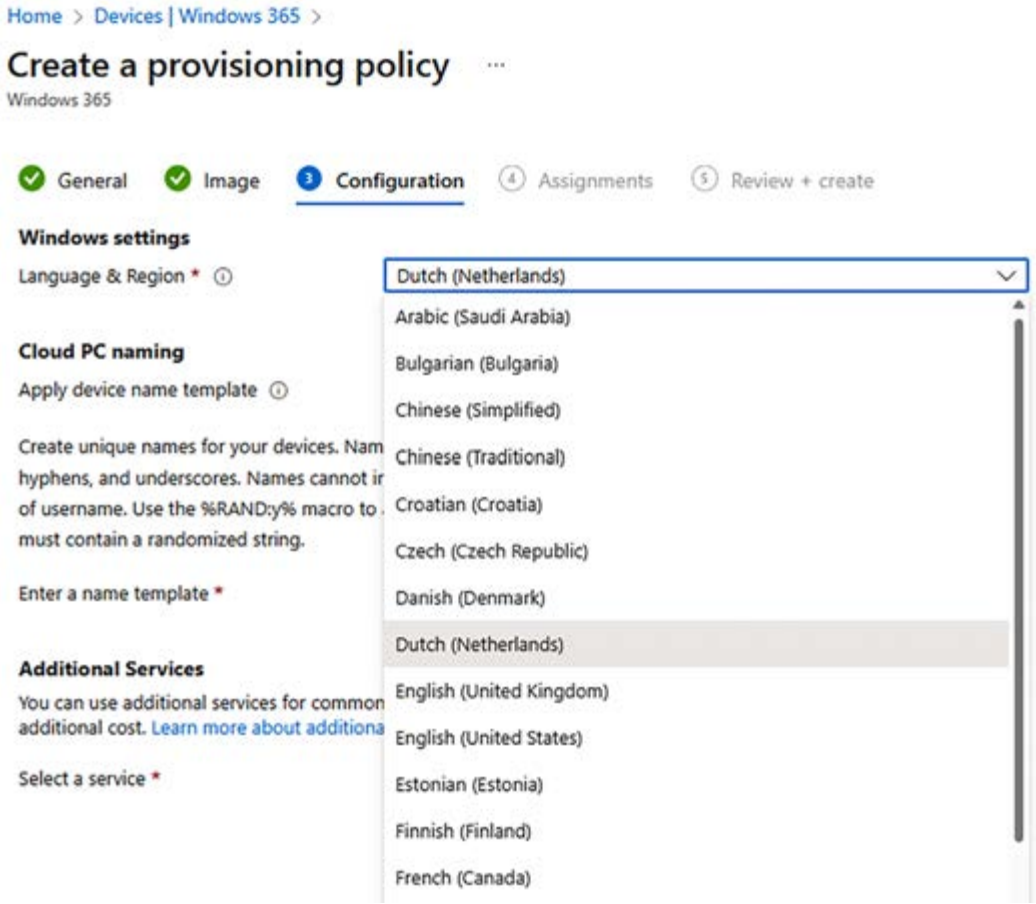


Figure 5.15: Language & Region

13. To create a Cloud PC naming template to use when naming all Cloud PCs that are provisioned with this policy, select Apply device name template. When creating the template, follow these rules:

    - Names must be between 5 and 15 characters
    - Names can contain letters, numbers, hyphens, and underscores
    - Names can't include blank spaces
    - Use the %USERNAME:X% macro to add the first X letters of the username (optional)

- Use the %RAND:Y% macro to add a random string of numbers, where Y equals the number of digits to add. Y must be 5 or higher. Names must contain a randomized string (required)

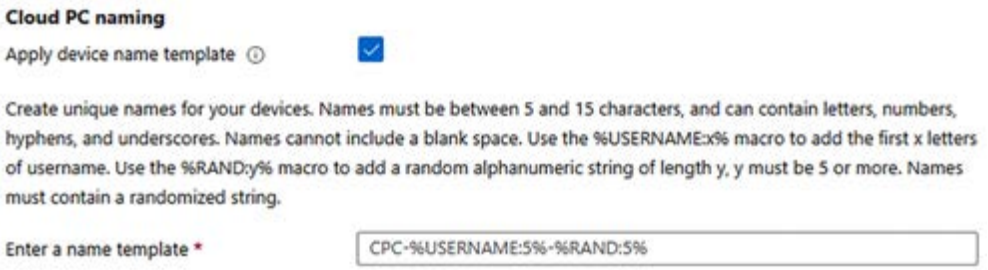


Figure 5.16: Cloud PC naming

14. Under additional services, you can select Windows Autopatch to let Microsoft take care of patching your Windows 365 Cloud PCs.
15. Selecting none requires that you manage the patching of your Windows 365 Cloud PCs using appropriate update, feature update, driver update, or quality update rings in Intune or via Configuration Manager if they are co-managed.

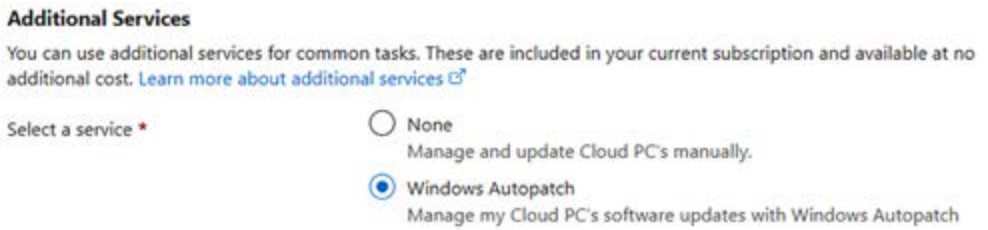


Figure 5.17: Select a service

16. Assign the Provisioning Policy to an Entra ID Group. Users in this group need to have appropriate Windows 365 licenses assigned.

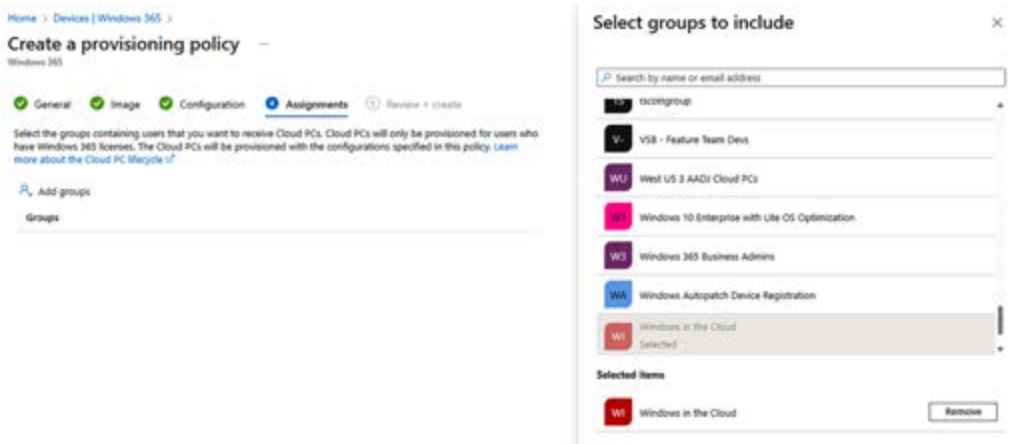


Figure 5.18: Select groups to include

17. Once you validated the settings you configured via the summary, click on **Create** to start the Cloud PC provisioning process. It takes around 30 – 40 seconds to finalize the provisioning of Cloud PCs depending on whether you are using Entra ID Join or Hybrid Entra ID Join Cloud PCs. Hybrid Entra ID Join Cloud PCs might take a little longer due to the replication time of the device within your Kerberos domain. Once the provisioning is done, you can log on to the Cloud PC via one of our designed apps and/or Windows-integrated experiences.

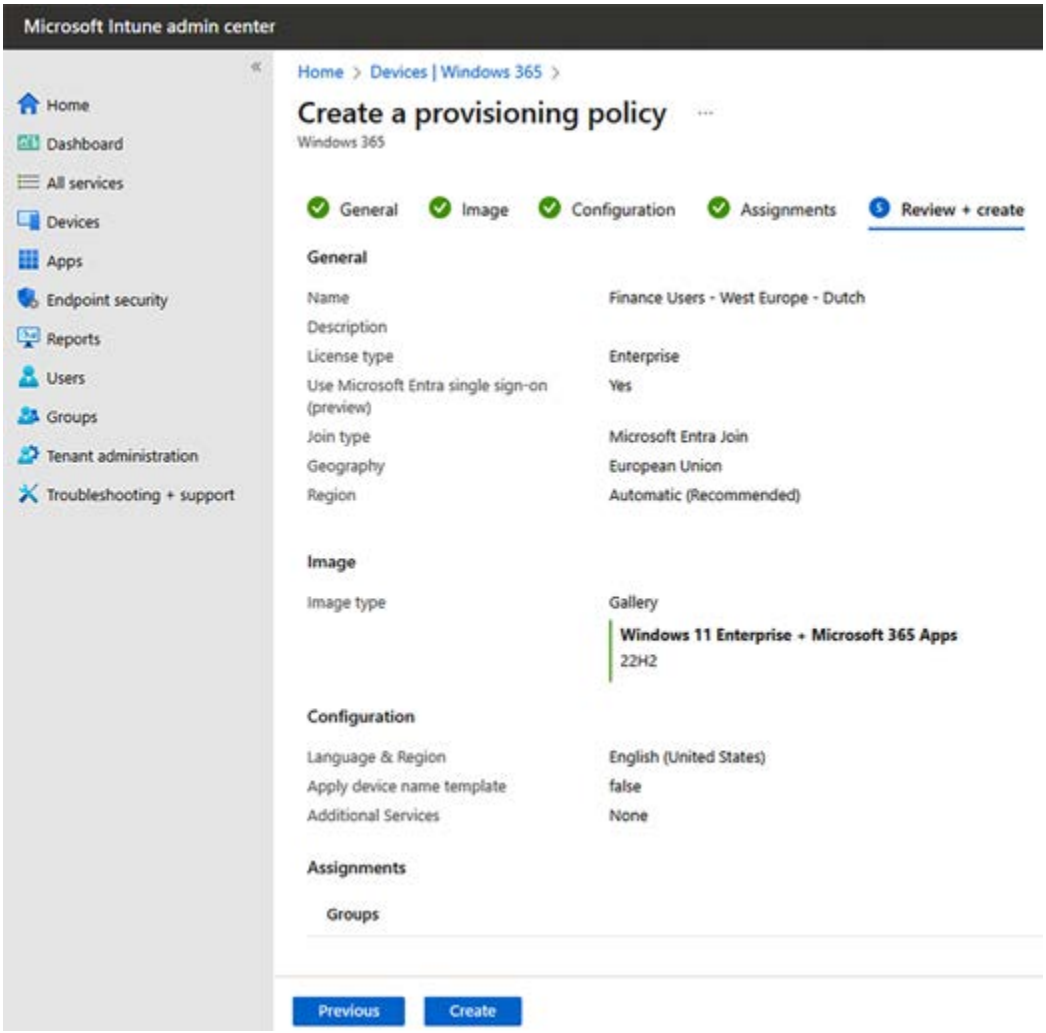


Figure 5.19: Review + create

Image management – creating a custom image (optional)

In traditional VDI environments, rolling out virtual desktops always starts with creating a custom image, also known as a **golden image**. Microsoft understands the need for this, which is why this approach is also supported in Windows 365.

However, the recommendation is to only use the custom image for baseline applications, agents, OS updates, and language packs. Then, you must target other configuration items and applications via Microsoft Intune just like you would target for physical devices. By leveraging Microsoft Intune for policy and application management, you will be more agile in your management strategy on your Cloud PCs.



IMPORTANT NOTE

This step is optional and is only required when you want to build your own custom images for use with Windows 365. Microsoft also provides Gallery images for both Windows 10 and Windows 11 that you can select during the provisioning policy creation process with Microsoft 365 Apps, Edge, and Teams optimizations pre-installed.

If you wish to build images before you start the Cloud PC provisioning process, perform the following steps:

1. Start at `https://portal.azure.com` and search for a Windows 365 Cloud PC image template.
2. Select a plan and click on **Create**:

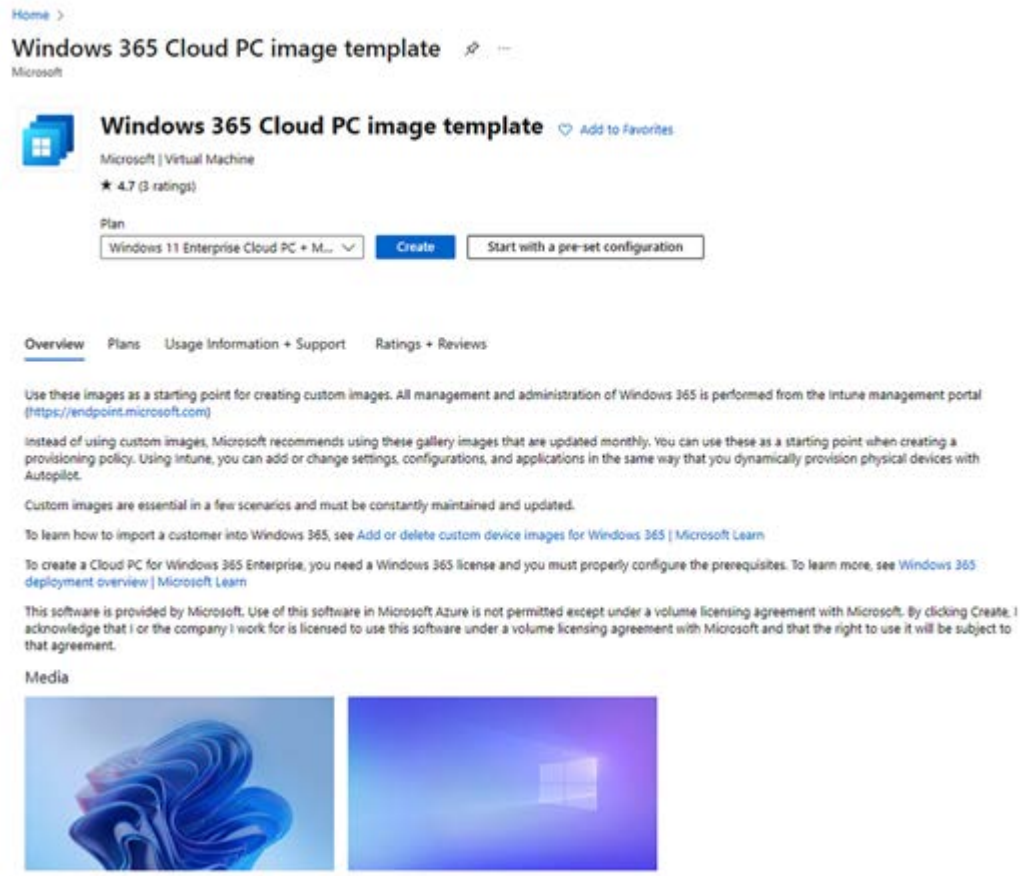


Figure 5.20: Building an image

3. Create a **virtual machine** (**VM**) image based on your specifics.
4. Select **Windows 10 Enterprise or Windows 11 – Gen**, as shown here:



IMPORTANT NOTE

Windows 365 supports Windows 10 Enterprise and Windows 11 single-session. Only select Windows 10 Enterprise multi-session when you want to create a custom image for Azure Virtual Desktop.

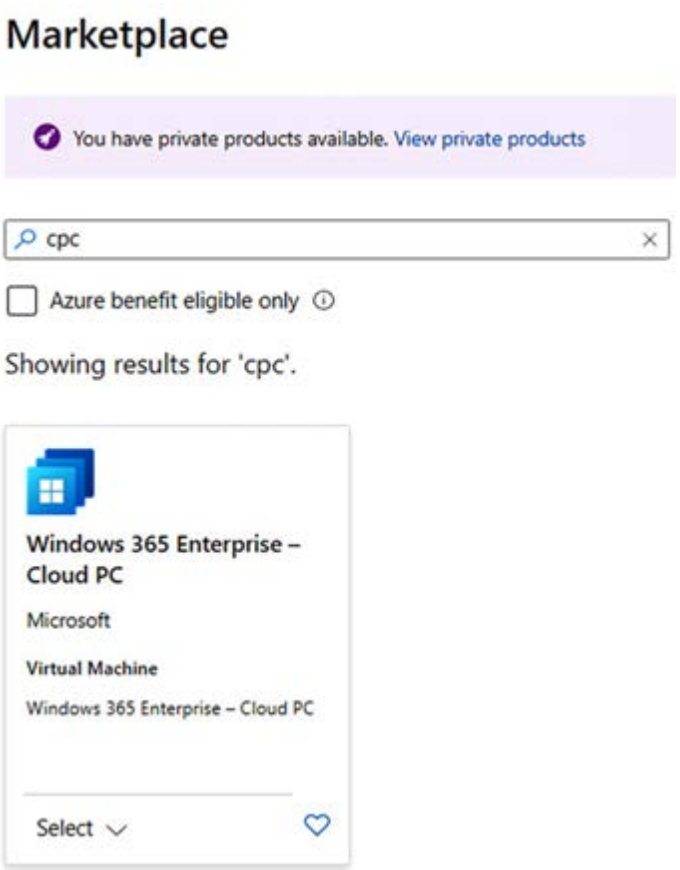


Figure 5.21: Cloud PC images

5. Fill in all the other properties and add the custom image to the right Azure VNet (standard SSD at a minimum) for proper performance.
6. In the **Advanced** tab, make sure **Gen 2** is selected for **VM generation**; for example, **Windows 10 Enterprise Cloud PC, Version 20H2 + Microsoft 365 Apps - Gen2:**

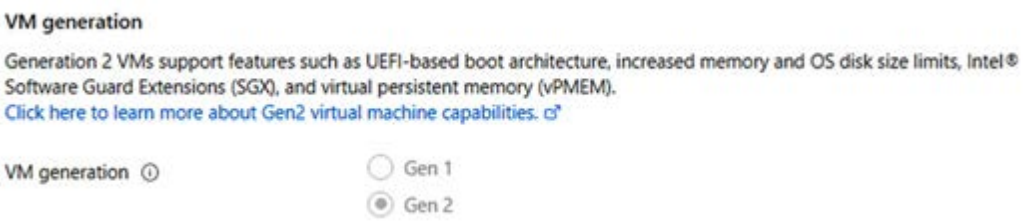


Figure 5.22: Advanced tab



IMPORTANT NOTE

Make sure that your image is created as Gen 2; Microsoft no longer supports adding new Gen 1 images as a part of Windows 365 Enterprise.

7. Click on **Review + create**:

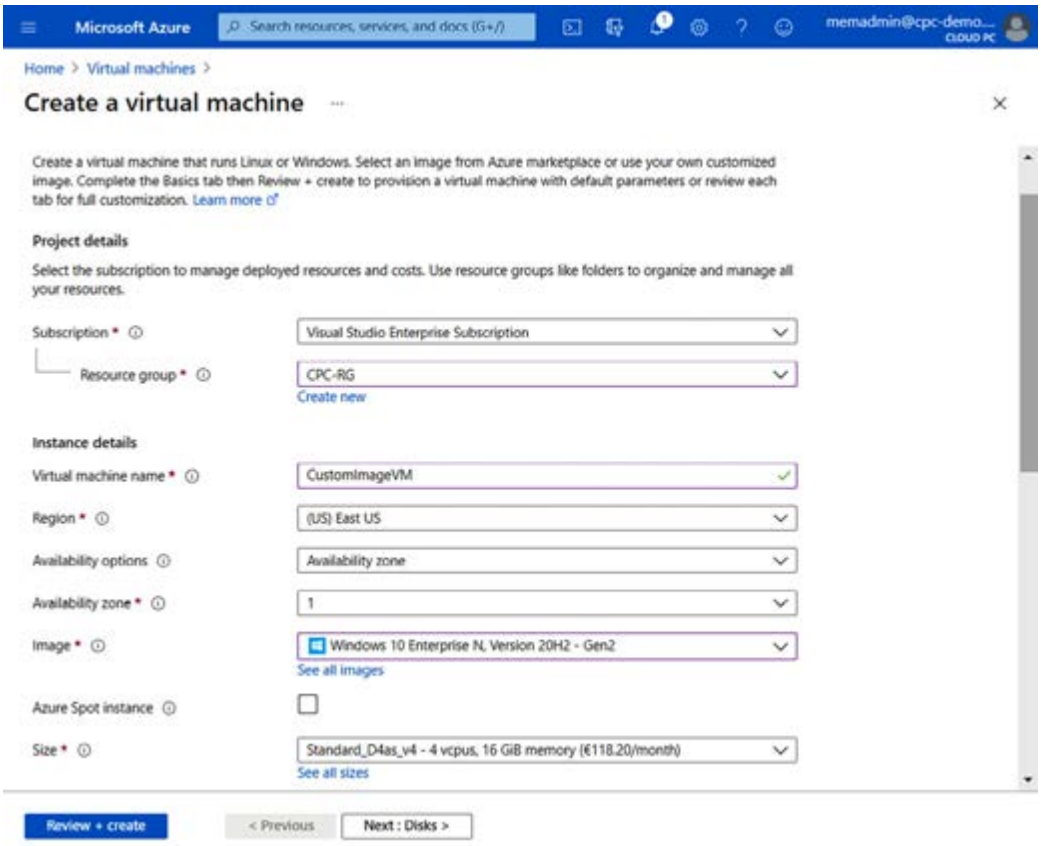


Figure 5.23: Reviewing your settings

8. Once the VM has been provisioned, use Azure Bastion or RDP to connect to the custom image VM. Read more about Azure Bastion on Microsoft Learn (`https://learn.microsoft.com/en-us/azure/bastion/bastion-overview`).
9. Install your agents and other software on the VM.



IMPORTANT NOTE

We recommend that you keep the image as clean as possible and add line-of-business apps via Microsoft Intune to make the image management process simple and modern. Microsoft also provides Microsoft 365 apps within pre-baked marketplace images.

10. Run **sysprep** via the **%WINDIR%\system32\sysprep\sysprep.exe /generalize /shutdown /oobe** command in the VM image.
11. Once you're ready, stop the VM by clicking on the **Stop** option, to put it in a stopped (de-allocated) state:

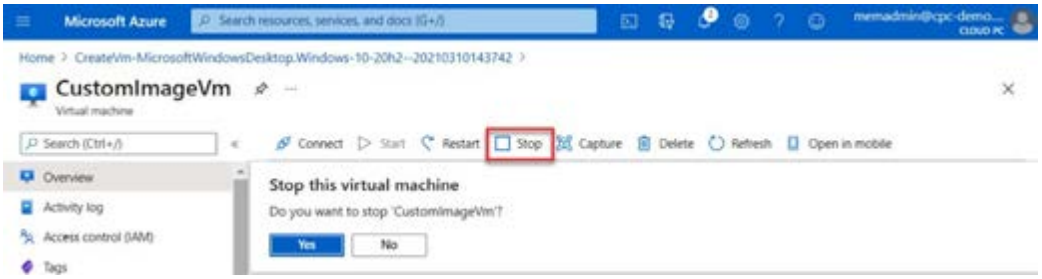


Figure 5.24: Stopping the VM

12. Click on the **Capture** button to start capturing the image:

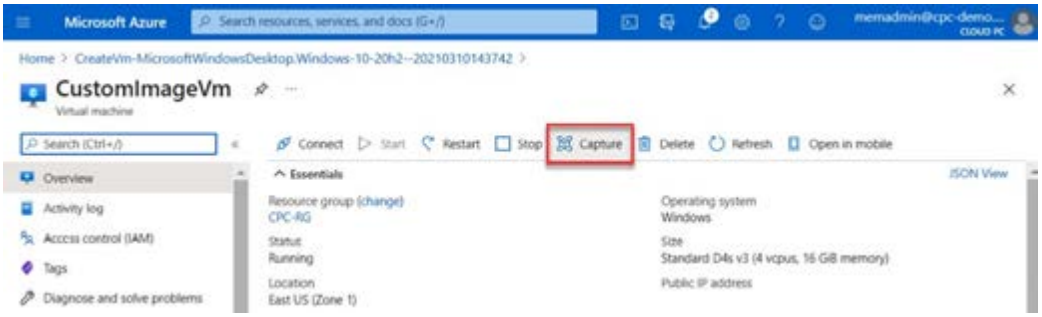


Figure 5.25: Capturing the image

13. Wait for the VM to change its status to **Stopped** (de-allocated). This takes around one minute to complete.

14. Select **No, capture only a managed image.** Then, click on **Review + create:**

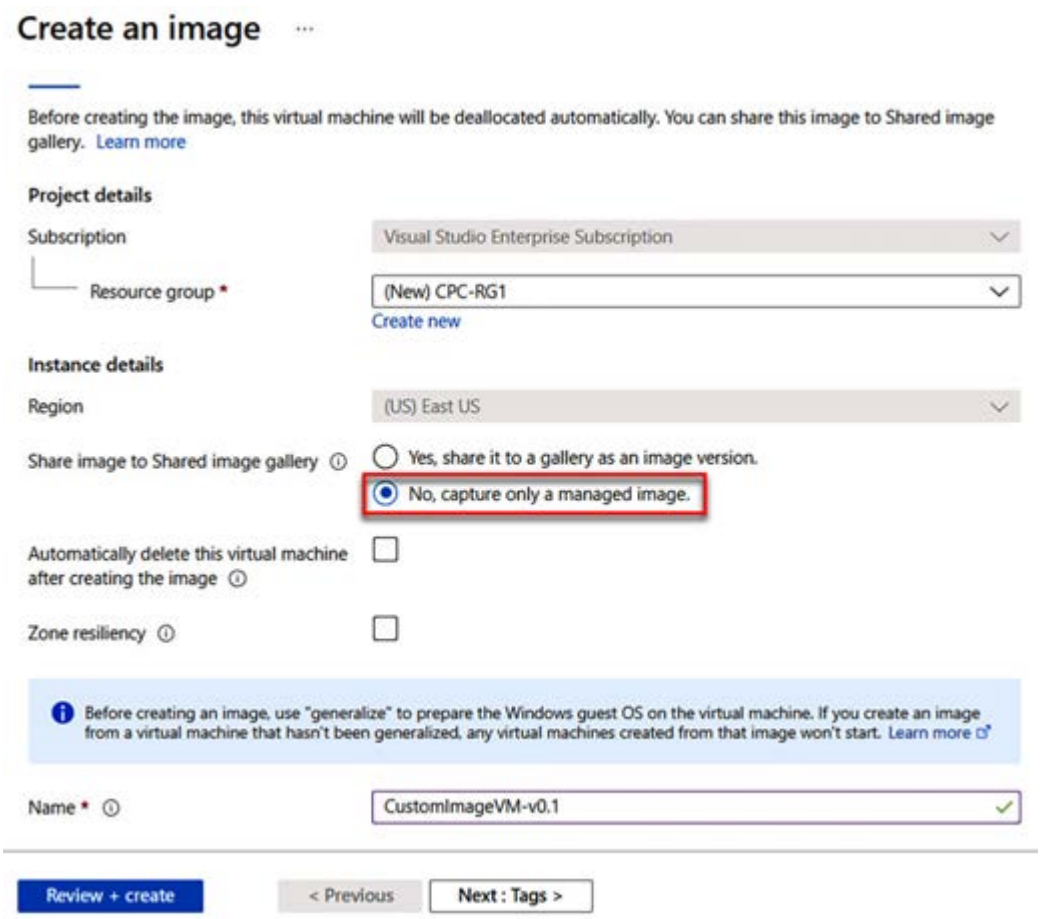


Figure 5.26: Reviewing your settings

15. Confirm the summary and click on **Create.** The process will now sysprep the image automatically:

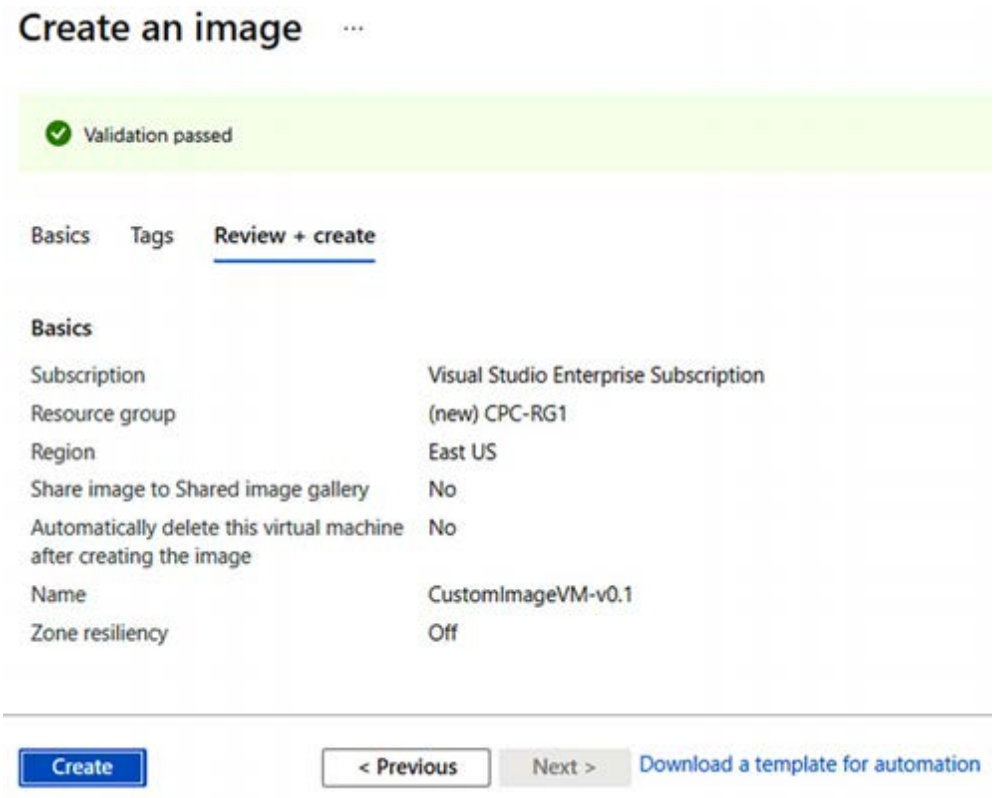


Figure 5.27: Successfully validated

The image will now be prepared. This process only takes a minute or so.

16. Once the process is ready, you can select your custom image under **Cloud PC – Provisioning policies** as a custom image in Windows 365.
17. Switch back to the Microsoft Intune admin center. Go to **Device images** and then click on **+ Add:**

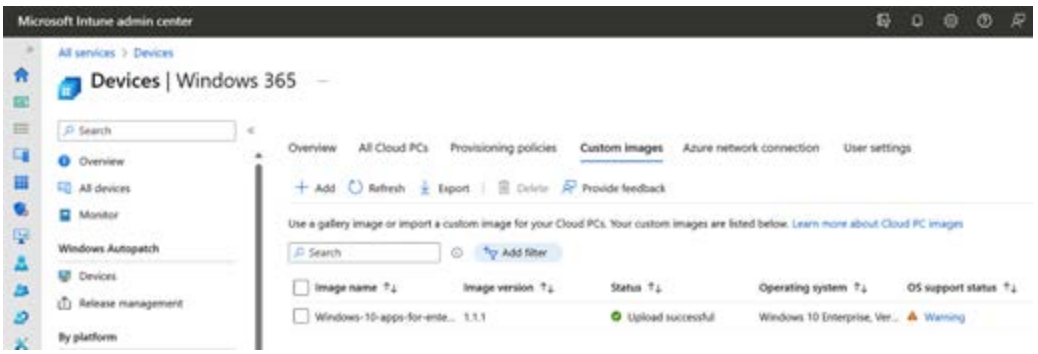


Figure 5.28: Adding an image

Provide the image's name, version, and the OS build version of Windows 10 Enterprise, as well as the source image.

18. Click on **Add**:

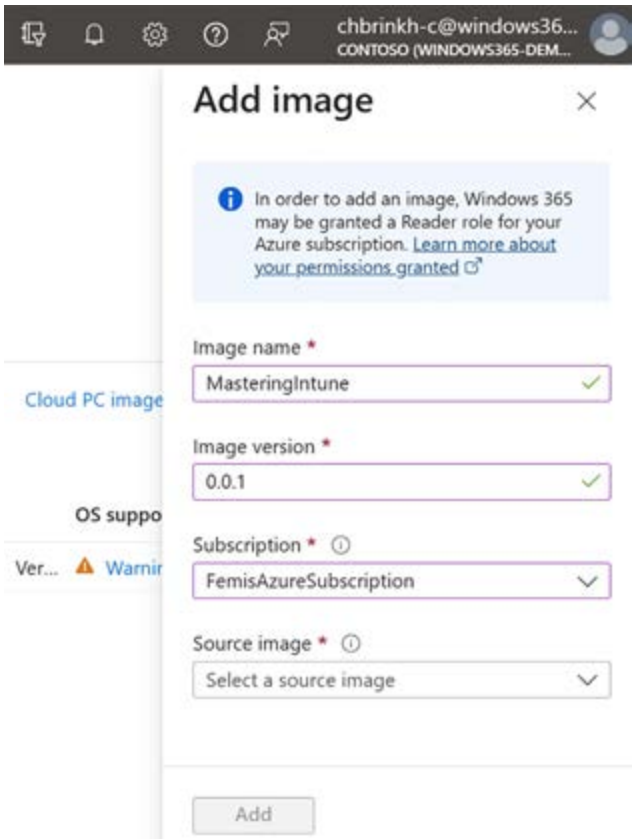


Figure 5.29: Uploading an image



IMPORTANT NOTE

The admin/service account adding the custom image needs contributor or owner role permissions on the storage account's storage blob container.

19. The image upload process will start. Once the process is complete, start creating the provisioning policy, or modify an existing policy.
20. When you update the image, any newly provisioned Cloud PCs will receive the new image. Existing Cloud PCs should initiate a reprovisioning task to get the updates.



IMPORTANT NOTE

Be aware of changing existing provisioning policies where users already have their Cloud PC provisioned. It's not possible to change the image from a marketplace image to a custom image. Your Cloud PC will enter a grace period.

You can update your images as much as you want as part of provisioning policies. All the new provisioned Cloud PCs will get the latest version, while the existing Cloud PCs must be triggered for reprovisioning. You learned how you can initiate this earlier in this chapter.

Reprovisioning a Cloud PC

You could also reprovision your Cloud PC via the **Reprovision** remote action; the user will be signed off and the Cloud PC will be deleted, including every application, all data, and customization that is done on the Cloud PC during the life time. Clicking it will initiate a reprovisioning process, meaning that it will start from scratch in the same way as you started it initially, without any customization needing to be installed on the Cloud PC.

You can find the **Reprovision** button under **Devices**, select a **Windows 365 Cloud PC** | **Overview** | **Reprovisioning**:

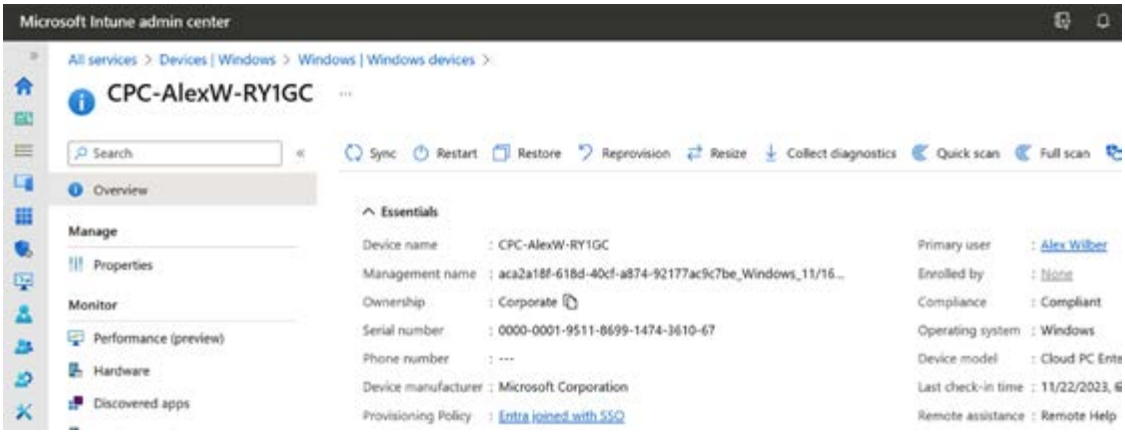


Figure 5.30: Reprovisioning your Cloud PC



IMPORTANT NOTE

You need (at least) Cloud PC administrator permissions to be able to do this. Reprovisioning takes some time, and the end user is not able to connect to the Cloud PC during this time.

IT admins will get the following prompt to confirm if they really want to reprovision the target Cloud PC as an extra safety check:



Figure 5.31: A prompt for the admin to confirm

Local administrator permissions

Within Windows 365 Enterprise, the Microsoft Intune version of managing Cloud PCs, users do not have local administrator rights out of the box. When you want all or some of your users to be local administrators, we can build the following feature into Microsoft Intune as a configuration profile under **Endpoint Protection | Account protection | Local user group membership** where you can configure the users that are being added to the local administrators group. This policy type is covered in depth in *Chapter 11*.

Make sure that you only configure the configuration profile for the devices or users that need these rights.

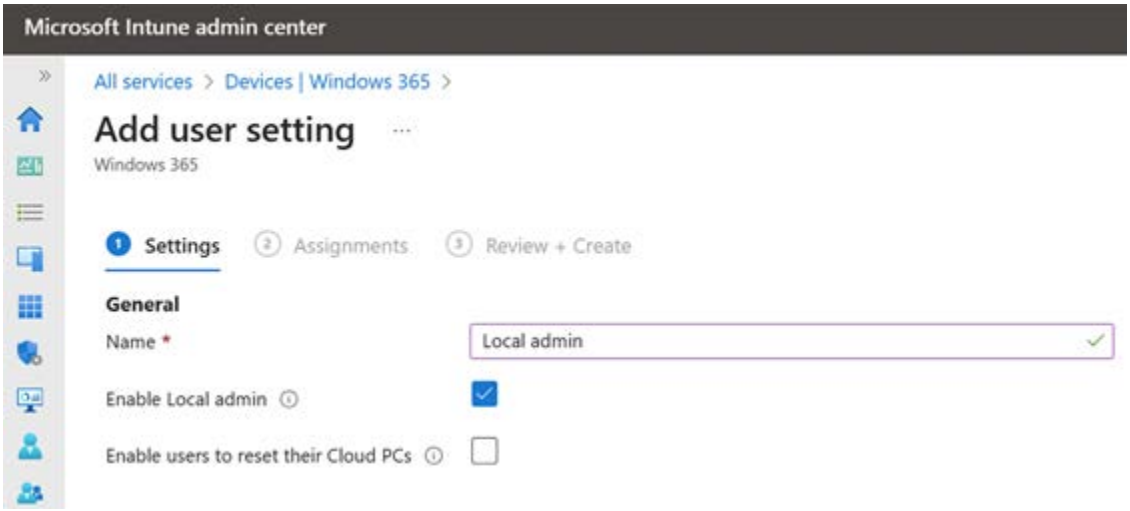


Figure 5.32: Enable Local admin

Security baselines for a Cloud PC

Using a virtualized desktop in the Microsoft Cloud requires a different security baseline than for physical Windows PCs, as some settings that require physical hardware are not currently present on a Cloud PC. Therefore, we created a new baseline optimized for Cloud PCs in the profile catalog.

Make sure that you select the Cloud PC security baseline for the best performance and security settings for your business:

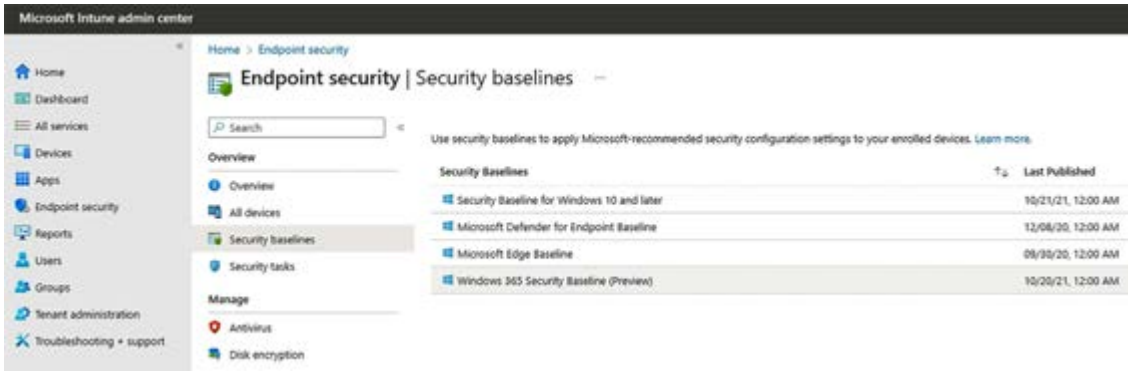


Figure 5.33: Selecting a Cloud PC security baseline

Zero Trust: Conditional Access management for Cloud PCs

It's essential to secure access to Cloud PC devices in your Windows 365 environment. One way to achieve this is by using **Conditional Access** (**CA**), which allows you to secure that environment based on specific conditions. We strongly recommend implementing **multi-factor authentication** (**MFA**) especially when accessing Cloud PCs from unknown locations, so end users need to provide more than just a username and password when they are off the corporate network. Additionally, you may want to consider using security keys based on **Fast Identity Online** (**FIDO**) for authentication as it provides phish-resistant credentials and frictionless logins as you would only need to either use a USB stick or NFC-based smartcards to log directly into your Cloud PC versus typing in your credentials!

Including a cloud app for Windows 365 and Azure Virtual Desktop in your CA policy helps secure all the different ways users are able to connect to their Cloud PCs. (Please note it might be called Windows Virtual Desktop instead of Azure Virtual Desktop in some Microsoft Entra ID tenants.)

Managing CA policies can be done in Microsoft Entra ID or in Microsoft Intune. The figure below shows Microsoft Intune, but the configuration is the same if you do it in Microsoft Entra ID.

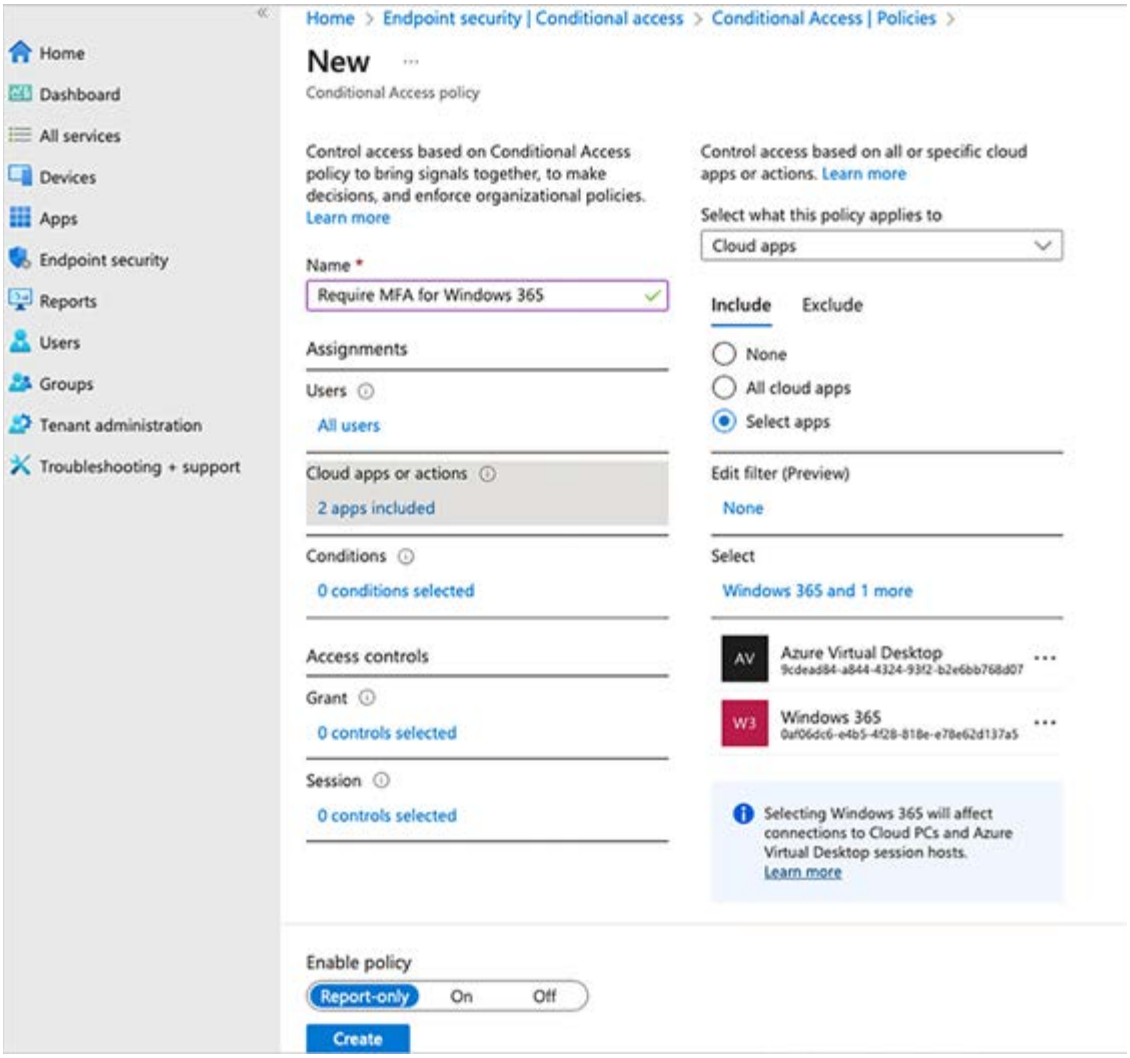


Figure 5.34: CA requires MFA for Windows 365

After activating this policy for your Cloud PCs, CA settings will apply and enforce MFA inside the Windows 365 app.



Figure 5.35: Verify your identity

Connecting to your Cloud PC

Windows App

Windows App is the new unified client application that connects Windows 365 Cloud PCs, Azure Virtual Desktop, Microsoft Dev Box, Remote Desktop Services, and RDP into one client end user experience.

Windows App is the replacement of the previous Windows 365 App. Windows App is designed with a customizable home screen to cater to your unique workflow needs. You can access your applicable Windows devices across multiple different services and remote PCs from a single place and pin the favorites you access most. If you use multiple accounts, you can easily switch between them with its easy account-switching feature.

There are many features to enhance your remote experience, such as:

- Multiple monitor support
- Open Remote Applications
- Custom display resolutions
- Dynamic display resolutions and scaling
- Device redirection, such as webcams, audio, storage devices, and printers
- Microsoft Teams optimizations

You can download Windows App from the Microsoft Store via the following link: `https://apps.microsoft.com/detail/9N1F85V9T8BN`

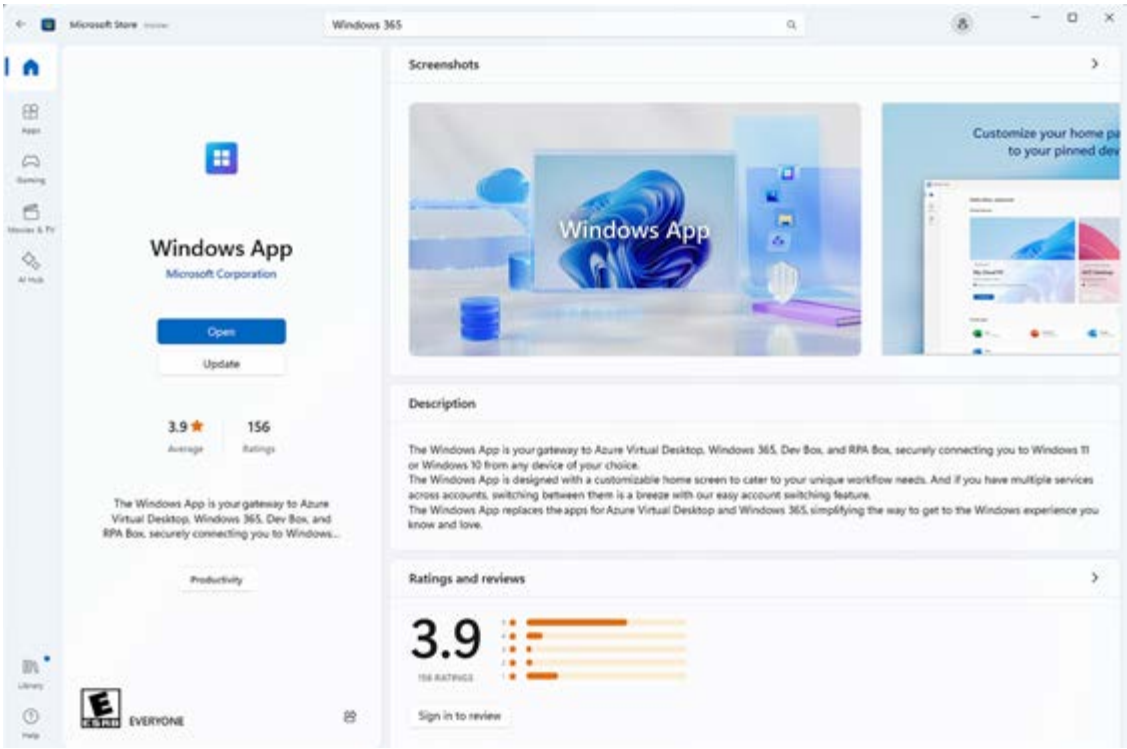


Figure 5.36: Windows App

After installing the app, open Windows App. If you already have the app installed, please open the application from the Windows start menu and/or search!

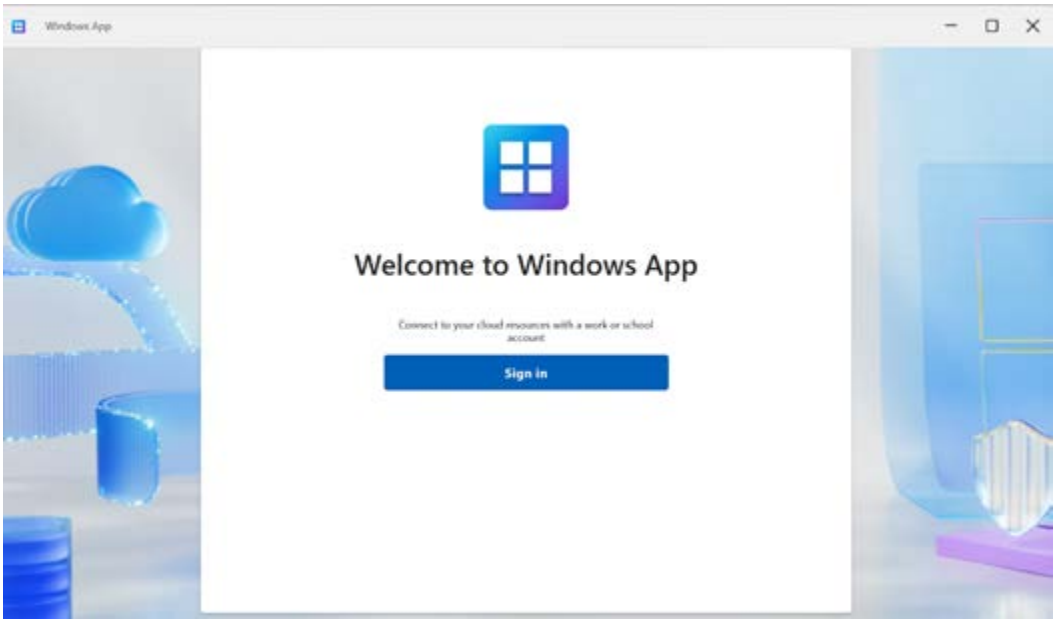


Figure 5.37: Windows App Sign in

Once you successfully sign in, the new user experience will be presented to the user.

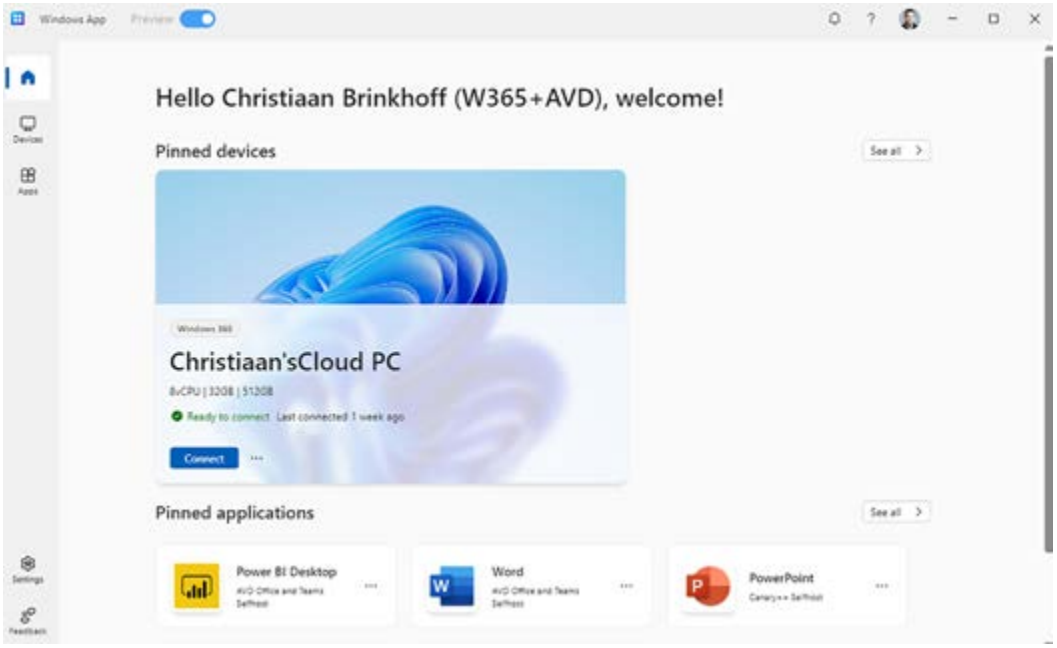


Figure 5.38: Windows App welcome page

Click on the **Connect** button to start the Cloud PC session in full screen.



Note: If you have multiple monitors and prefer a different setup of displays and such, you will be able to change this in the app under the Cloud PC settings menu that you can find under the ellipsis.

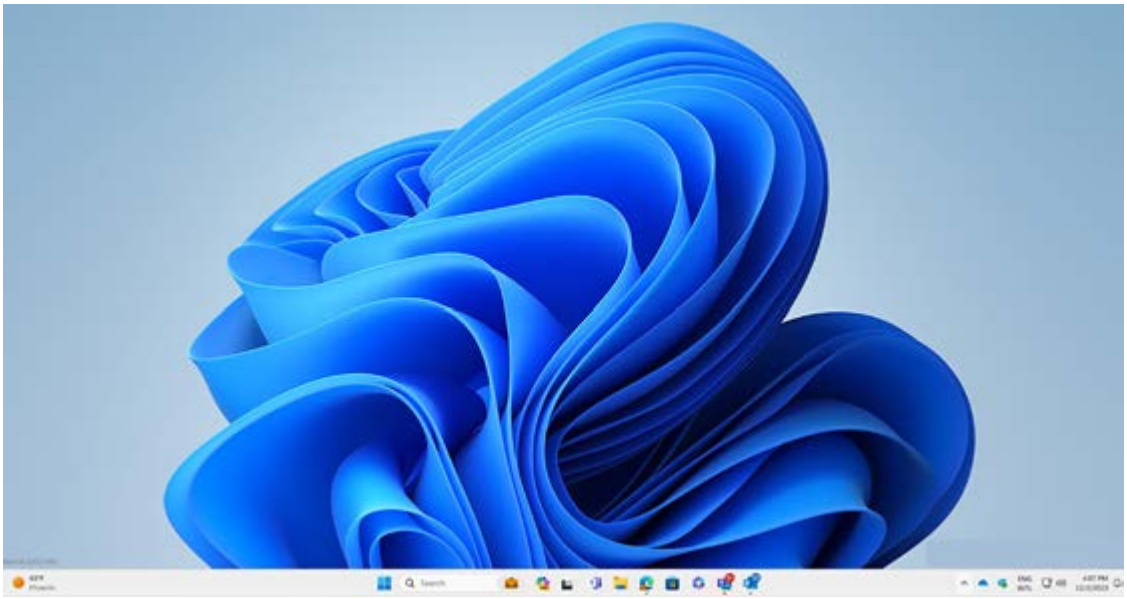


Figure 5.39: Windows 365 desktop

Windows App also includes a configuration menu called **Settings**, highlighted in the following figure, to change display configuration settings, dark or light mode, and more. Click on the **ellipsis** beside **User Actions**, to start the configuration.

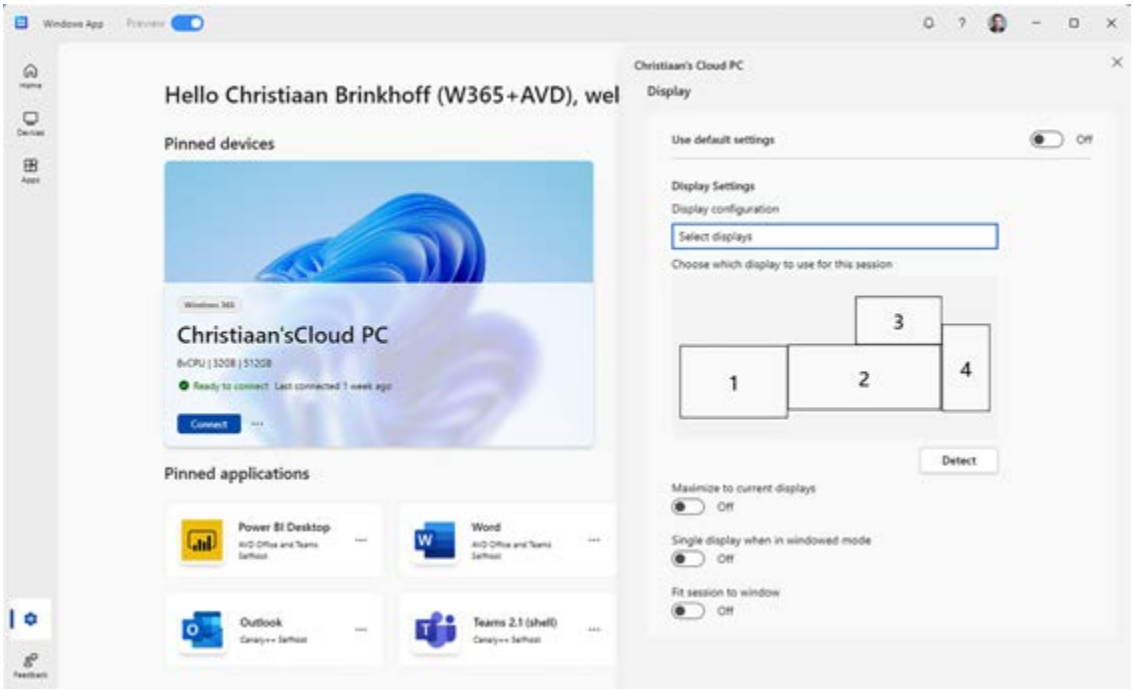


Figure 5.40: Windows App configuration settings

Deploy Windows App via Intune

If you want to deploy Windows App to Windows 10 or Windows 11 endpoints on a bulk basis, we recommend you use the new Microsoft Store app deployment option in Microsoft Intune, as it can be silently deployed to your end users' devices either in a device or user context.



Note: We will go deeper into Enterprise App Deployment later in the book.

1. To use the app enrolment option in Intune, go to **Apps** and select Microsoft Store app (new).

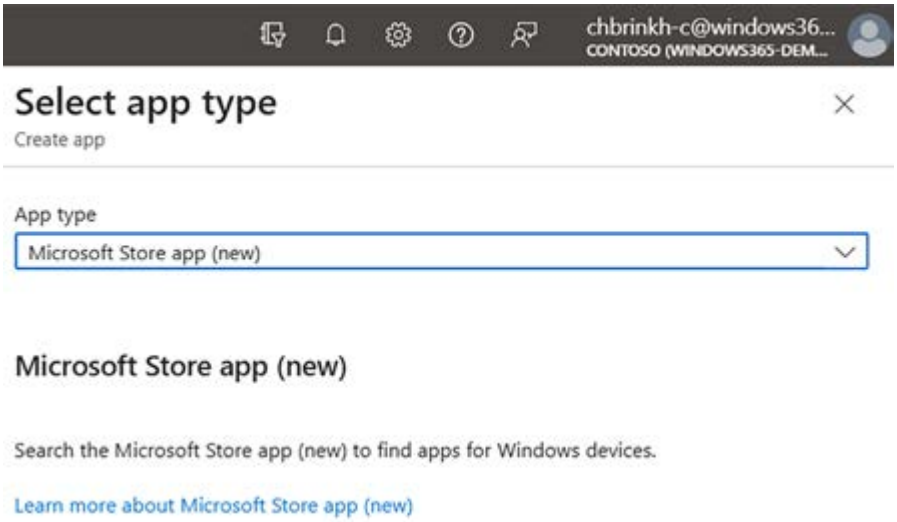


Figure 5.41: Microsoft Store app (new)

2. Search for **Windows App**.

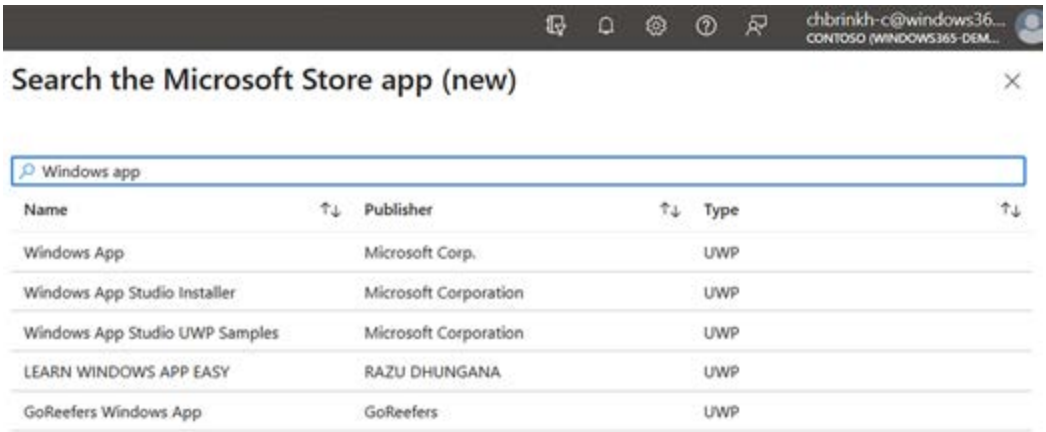


Figure 5.42: Search Windows App

3. Finish the app configuration, as per your own needs.

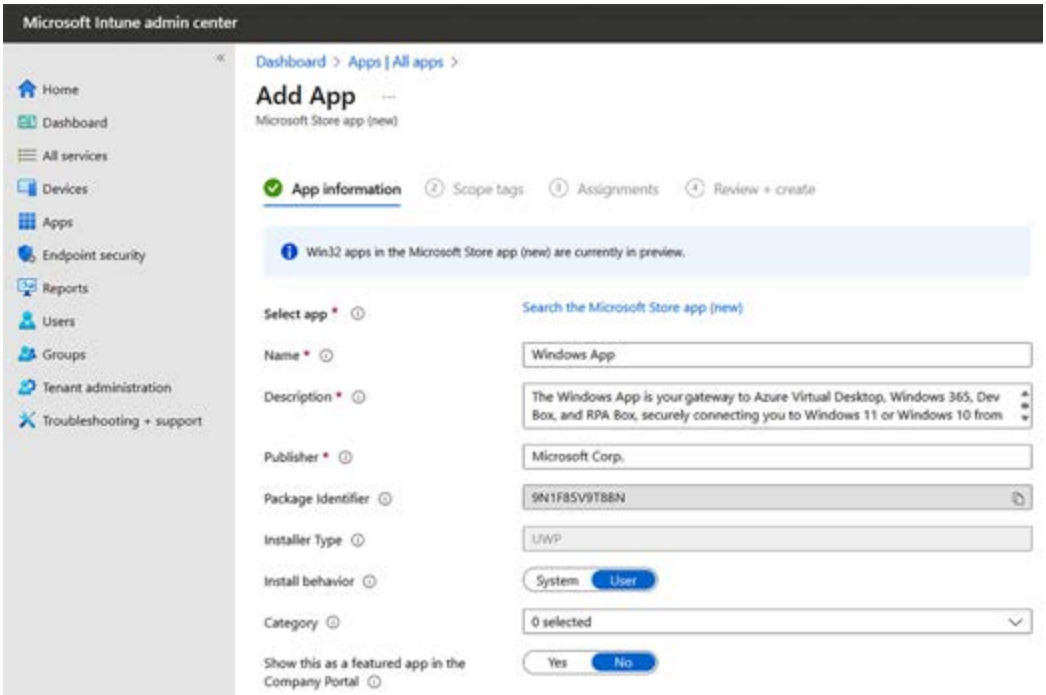


Figure 5.43: App information – Windows App

4. Assign the app enrolment to your Entra ID group that includes the users (installs per user that signs in to the device) or devices (installs once per device) that should receive Windows App.

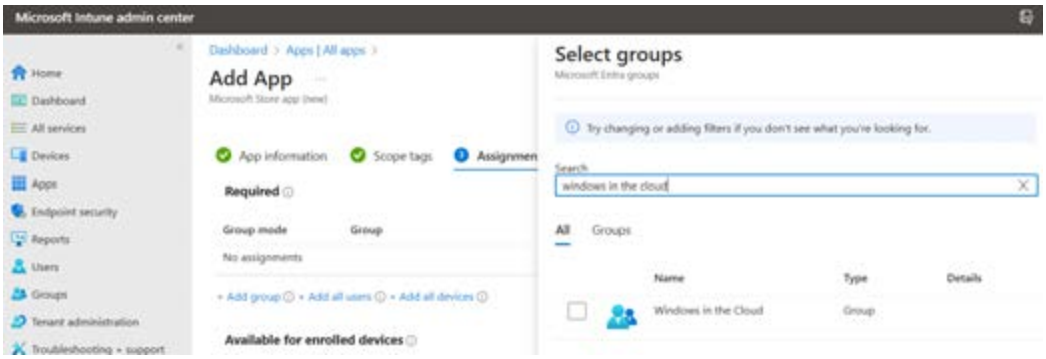


Figure 5.44: Assignment – Windows App

Windows App – User Actions

Reducing the burden of work on your IT support department and IT admins is the main goal when using the self-service options within Windows 365. When users have permissions for self-service actions (as shown in the following screenshot), they can perform reboots of their Cloud PC, as well as upgrade to larger VMs for better performance that fits their needs:

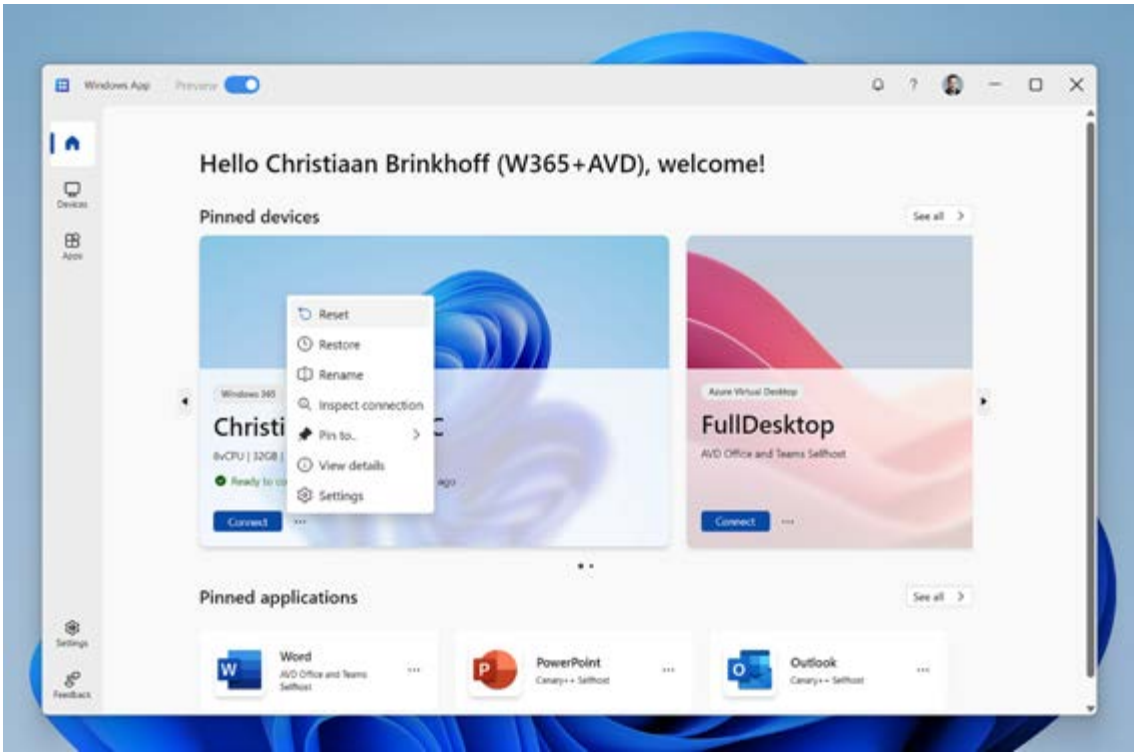


Figure 5.45: Windows App – self-service user settings

Self-service upgrades allow users to upgrade the performance and storage capacities of their Cloud PCs without admin approval. This will *NOT* incur any additional costs for your organization. The next section will go over the supported actions for the IT admin.

Bulk User Actions via Intune

From within Microsoft Intune's **Devices** menu, IT admins can reboot Cloud PCs remotely. The **Restart** button, which sits next to the **Sync** button to enforce MDM policy settings to the Cloud PC, could also be a useful setting to provide.

Supported redirections per endpoint platform

You can access your Cloud PCs via Windows via the new Windows App. There are also other clients available for mobile platforms and other operating systems such as MacOS, and Linux client support is provided via partners such as IGEL and 10Zig, and users can use the new Windows App web portal on Linux today as well!

The following table explains the differences between the different endpoints that are supported for Windows 365 at the time of writing:

Connect to/from	Windows	macOS	iOS/iPadOS	Web browser
Azure Virtual Desktop	✓	✓	✓	✓
Windows 365	✓	✓	✓	✓
Microsoft Dev Box	✓	✓	✓	✓
Remote Desktop Services	✗	!	!	✗
Remote PC	✗	!	!	✗

Figure 5.46: Windows App Connect to/from table

Windows effects configuration

The following table shows the differences per platform for display features.

Feature	Windows	macOS	iOS/iPadOS	Web browser
Appearance (dark or light)	✓	✓	✓	✓
Integrated apps	✓	✓	✗	✗
Localization	✓	✗	✗	✓
Pin to home	✓	✓	✓	✓
Search	✓	✓	✓	✓
Uniform Resource Identifier (URI) schemes	✓	✗	✗	✗

Figure 5.47: Windows effects configuration

Display configuration

The following table shows the differences per platform for display features.

Feature	Windows	macOS	iOS/iPadOS	Web browser
Dynamic resolution	✓	✓	✗	✓
External monitor	✓	✓	✓	✗
Multiple monitors[1]	✓	✓	✗	✗
Selected monitors	✓	✗	✓	✗
Smart sizing	✓	✓	✗	✗

Figure 5.48: Windows display configuration

Multimedia redirection

The following table shows the differences per platform for media redirection features.

Feature	Windows	macOS	iOS/iPadOS	Web browser
Multimedia redirection	✓	✗	✗	✗
Teams media optimizations	✓	✓	✗	✗

Figure 5.49: Windows multimedia redirection

Device redirection

The following table shows the differences per platform for device redirection features.

Device type	Windows	macOS	iOS/iPadOS	Web browser
Cameras	✓	✓	✓	✓[1]
Local drive/storage	✓	✓	✓	✓[2]
Microphones	✓	✓	✓	✓
Printers	✓	✓[3]	✗	✓[4]
Scanners	✓	✗	✗	✗
Smart cards	✓	✓	✗	✗
Speakers	✓	✓	✓	✓

Figure 5.50: Windows device redirection

Ports redirections

The following table shows the differences per platform for port redirection features.

Port type	Windows	macOS	iOS/iPadOS	Web browser
Serial	✓	✗	✗	✗
USB	✓	✗	✗	✗

Figure 5.51: Windows ports redirection

Other redirections

The following table shows the differences per platform for other redirection features.

Feature	Windows	macOS	iOS/iPadOS	Web browser
Clipboard - bidirectional	✓	✓	✓[1]	✓
Clipboard - unidirectional	✗	✓	✗	✗
Location	✓[2]	✗	✓	✓
Third-party virtual channel plugins	✓	✗	✗	✗
Time zone	✓	✓	✓	✓
WebAuthn	✓	✗	✗	✗

Figure 5.52: Windows other redirection

Identity redirections

The following table shows the differences per platform for identity redirection features.

Credential type	Windows	macOS	iOS/iPadOS	Web browser
FIDO2 security keys	✓	✗	✗	✓
Microsoft Authenticator	✓	✓	✓	✓
Password	✓	✓	✓	✓
Smart card with Active Directory Federation Services	✓	✓	✗	✓
Smart card with Microsoft Entra certificate-based authentication	✓	✓	✓	✓
Windows Hello for Business certificate trust	✓	✗	✗	✓[1]
Windows Hello for Business cloud trust	✓	✗	✗	✓[1]
Windows Hello for Business key trust	✓	✗	✗	✓[1]

Figure 5.53: Windows identity redirection

This makes it easier for you to adjust the device based on the requirements for redirection. We're constantly improving the clients, so there's a high chance that some features will be supported when you start reading this book.

Windows 365 Boot shared mode

Windows 365 Boot is one of the newest Windows integrations released as part of Windows 365 and Windows 11. The feature allows users to boot directly to Cloud PCs from the initial Windows login screen. The feature allows users to sign in to their Windows 365 Cloud PC directly from a physical device running Windows. This is useful for shared PC scenarios, where users can access their own personal and secure Cloud PC without signing in to the physical device itself. To use Windows 365 Boot, IT administrators need to configure the physical devices and push the Windows 365 Boot settings to them with Intune. This means that the pain of logging on to a local Windows PC first, opening Windows App, and clicking connect, has completely vanished!

In this section, we will be explaining how you can push the Windows 365 Boot components to your Windows 11 endpoints via Microsoft Intune via a simplified guided flow scenario that is purposely built for this feature. Let us get started:

1. Go to **Devices** | **Device onboarding** | **Windows 365** and open the Boot to Cloud PC guide.
2. You are forwarded to the Boot to Cloud guided flow scenario, which involves all the configuration steps to enable Windows 365 Boot via 5 simple steps!

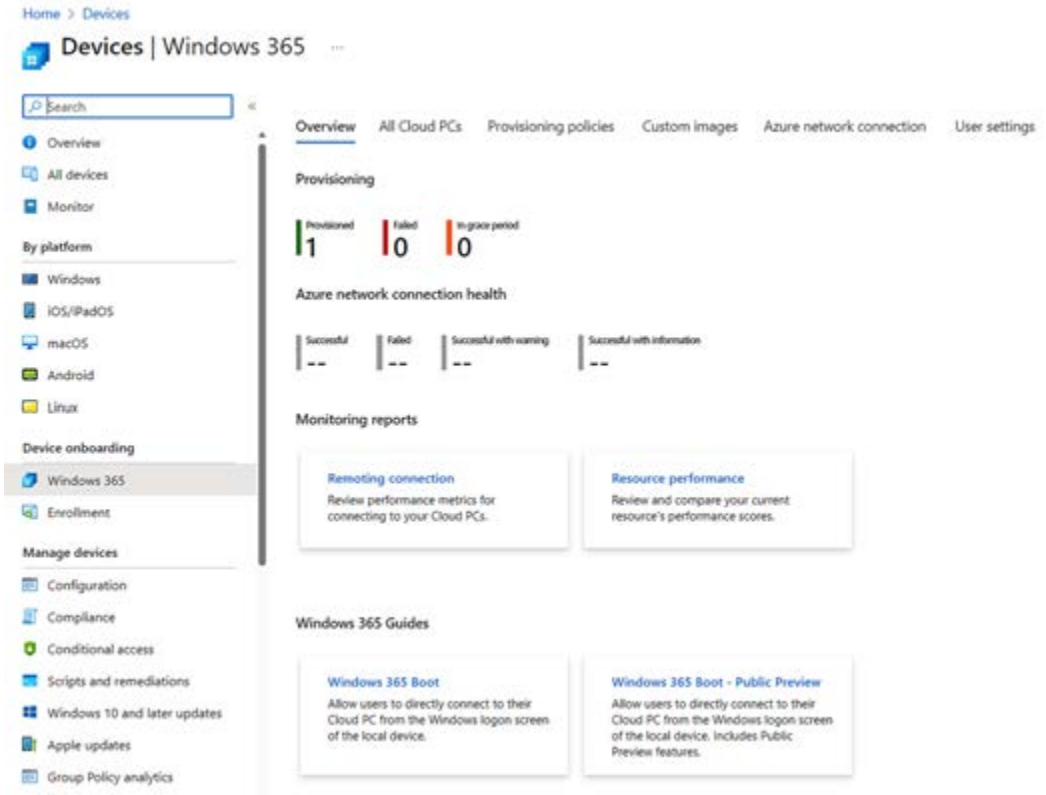


Figure 5.54: Windows 365 Boot



Note: To move forward, you need to have at least Group and Intune Administrator rights.

3. Click on **Next: Basics** to start the configuration.

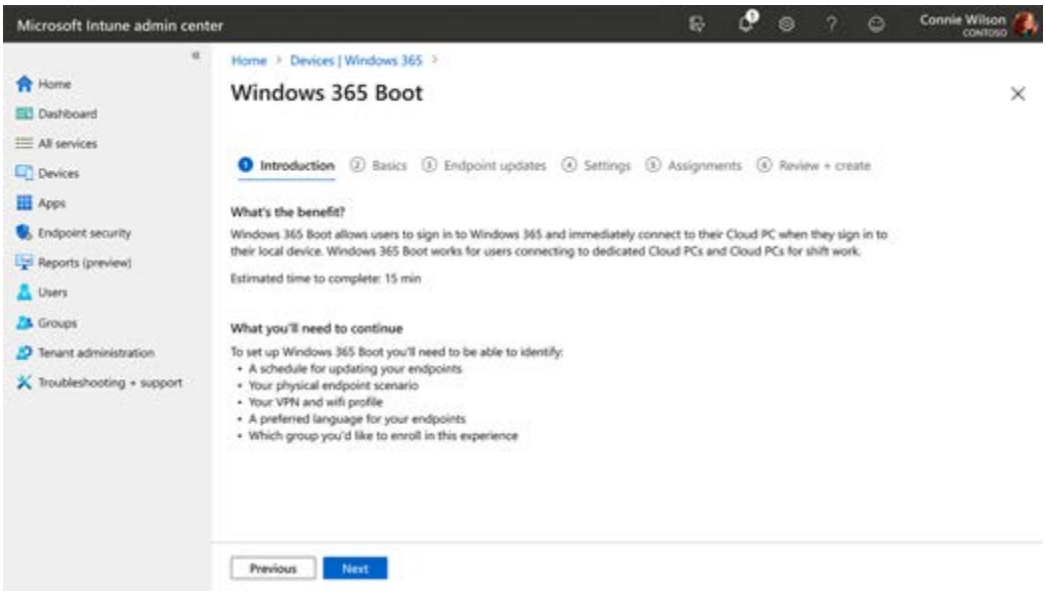


Figure 5.55: Microsoft Intune Boot to Cloud PC guide



Note: The following setting is optional but can be extremely useful to rename your endpoints to start with something such as BTC for Boot to Cloud PC to identify endpoints remotely.

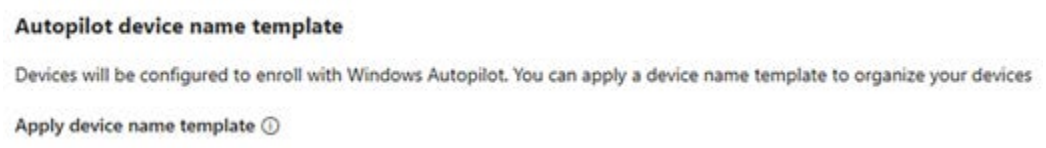


Figure 5.56: Autopilot device name template

4. Enter a **Resource** prefix name. This is useful for identifying the resources created if you need to modify them.
5. Decide on the Windows 365 Boot mode:
    a. **Shared PC mode:** The physical boot device will be shared by multiple users to connect to their individual Cloud PCs. *This is a very convenient scenario to combine with Windows 365 Frontline users!*
    b. **Dedicated User Mode:** The physical boot device will be assigned to a specific user to connect to their Cloud PCs.

During setup, the following resources are created:

- <prefix> Windows App
- <prefix> ESP
- <prefix> Autopilot profile
- <prefix> Device Configuration
- <prefix> AAD group

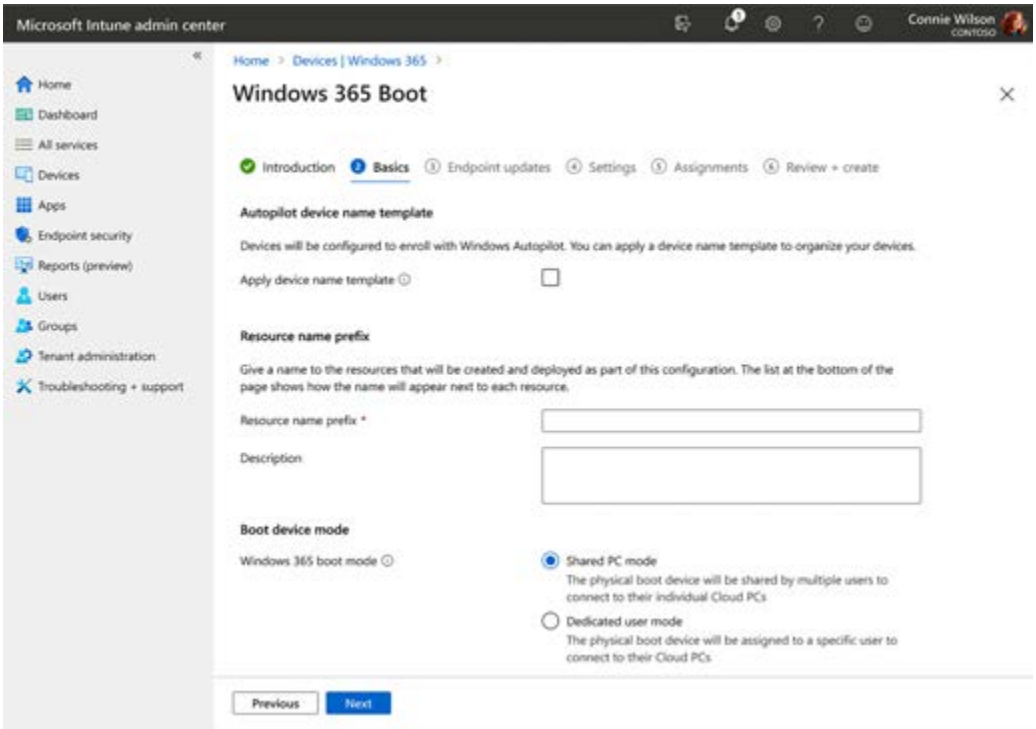


Figure 5.57: Resource prefix name

6. The following settings are all related to **Windows Updates**. As there is no local Windows UI/shell available to the user, and it is a shared PC, it is important that you ensure that Windows remains secure proactively.



Note: Windows 365 Boot also supports Windows Autopatch to prevent you from doing patch management on the Boot to Cloud endpoint.

7. The first setting ensures that updates are being applied after they are released during, for example, Patch Tuesday.
8. The second setting provided the option to add working hours to when a restart can apply to not disturb the productivity of the end user.
9. The last setting is to ensure updates are being installed and applied in a certain amount of time to ensure your end users are always using Windows secure when connecting to their Cloud PC.

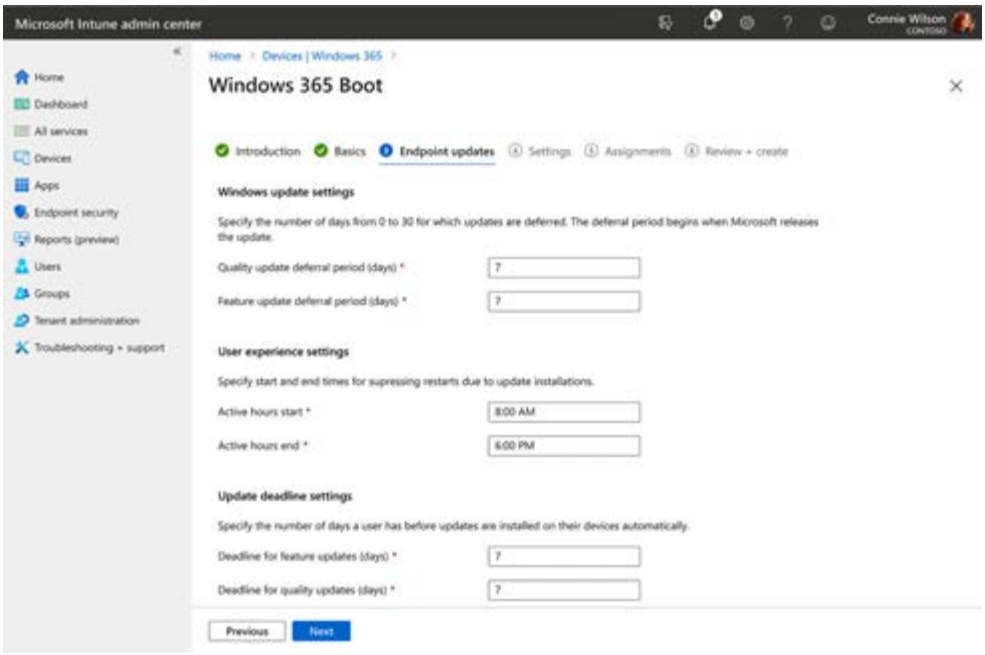


Figure 5.58: Endpoint update settings

10. Once ready with your Windows Updates preferences, you can **pre-configure VPN** and **Wi-Fi profiles** to push to the endpoint. This setting is optional.
11. The **language** setting is to provide the **local language** you prefer to use on the endpoint (e.g., for the Windows logon screen). All languages that Windows 11 supports are configurable.

12. You can enable the company logo and name branding in Microsoft Intune – you can find the changes under the **Settings** menu.

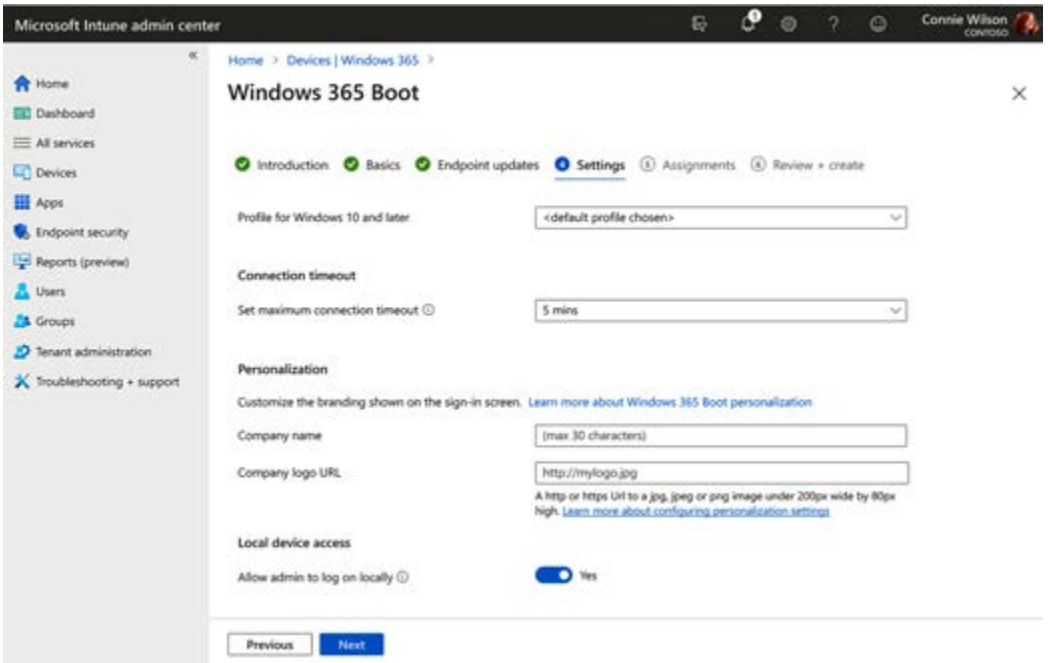


Figure 5.59: Networking and Language settings

13. The last setting is simple: you must either **create** or **assign** an existing Entra **ID group** to the set of resources to assign to.



Figure 5.60: User assignments

14. Check all your **settings** on the summary page and proceed.



Note: We recommend assigning the settings to Windows 11 endpoints that received a wipe or just came out of the box. If you deploy Windows 365 Boot to existing Windows 11 endpoints, we recommend that you remotely wipe the endpoint after finishing this configuration, so the device will get all the configurations and not have any settings and applications left over from previous use of the device.

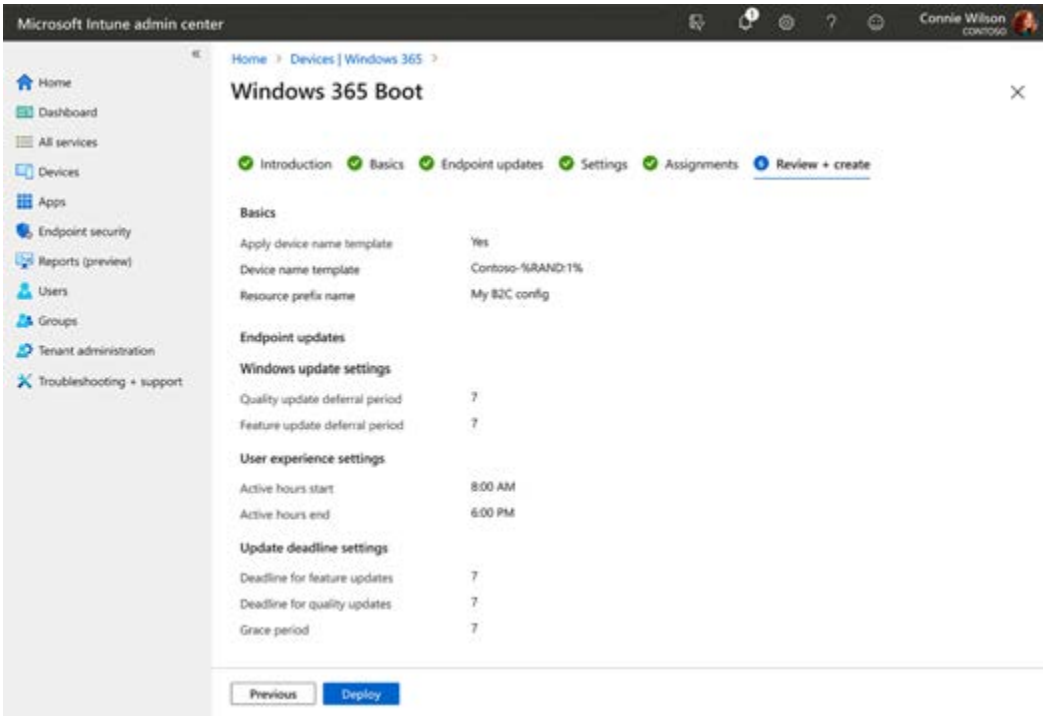


Figure 5.61: Summary page

Once ready, all your endpoints in the Entra ID group you either attached or created new will get the resources assigned and transform into Boot to Cloud mode in a couple of hours.

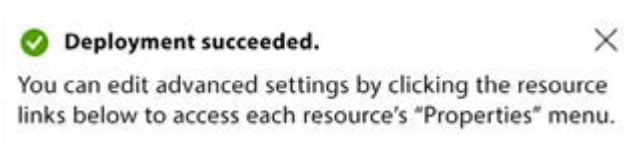


Figure 5.62: Deployment succeeded notification

Once the machine is ready, the device is ready to Boot directly into a Cloud PC. The user's lock screen is the same as for Windows 11 Pro and Enterprise.



Figure 5.63: Boot directly into a Cloud PC

15. Once you unlock the screen, the user needs to type in the credentials.

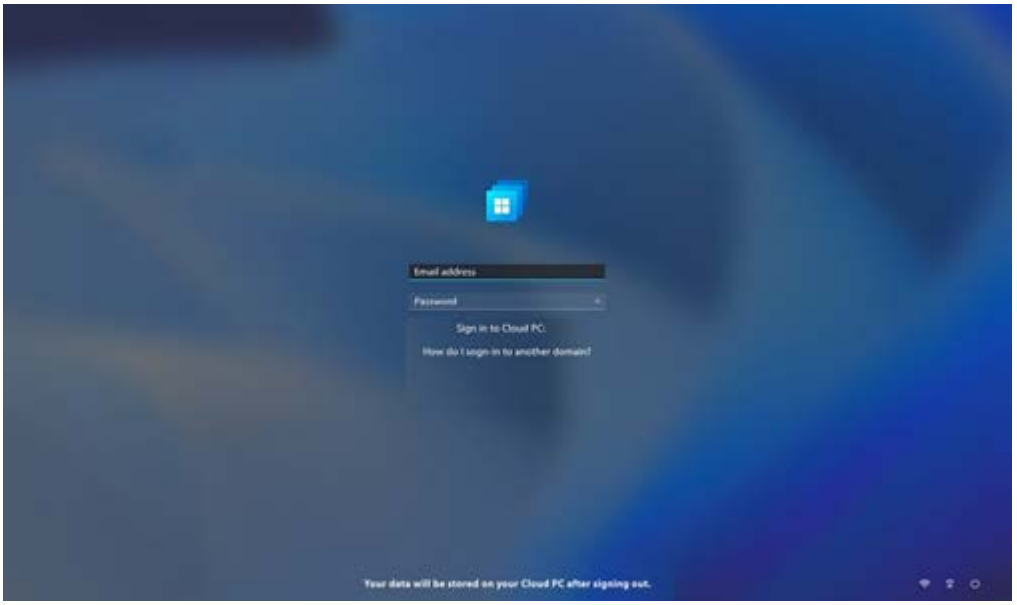


Figure 5.64: Cloud PC sign in

16. Once the credentials are validated, the user will log on to the Cloud PC via a new modern logon UI experience!

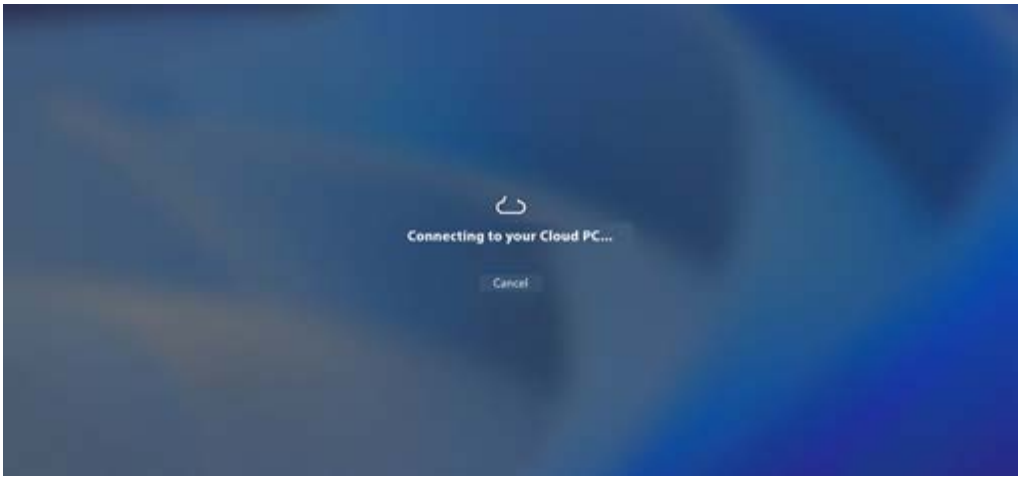


Figure 5.65: Connecting to your Cloud PC

The user will complete logging on when the Windows 365 Bloom wallpaper is visible and the new connection bar interface appears.

The other great thing is that when the user logs off from within the Cloud PC, the state of the Cloud PC will reflect the local Windows logon screen, meaning that the user can directly log on again, or another user that wants to use the same machine to connect to a different Cloud PC.

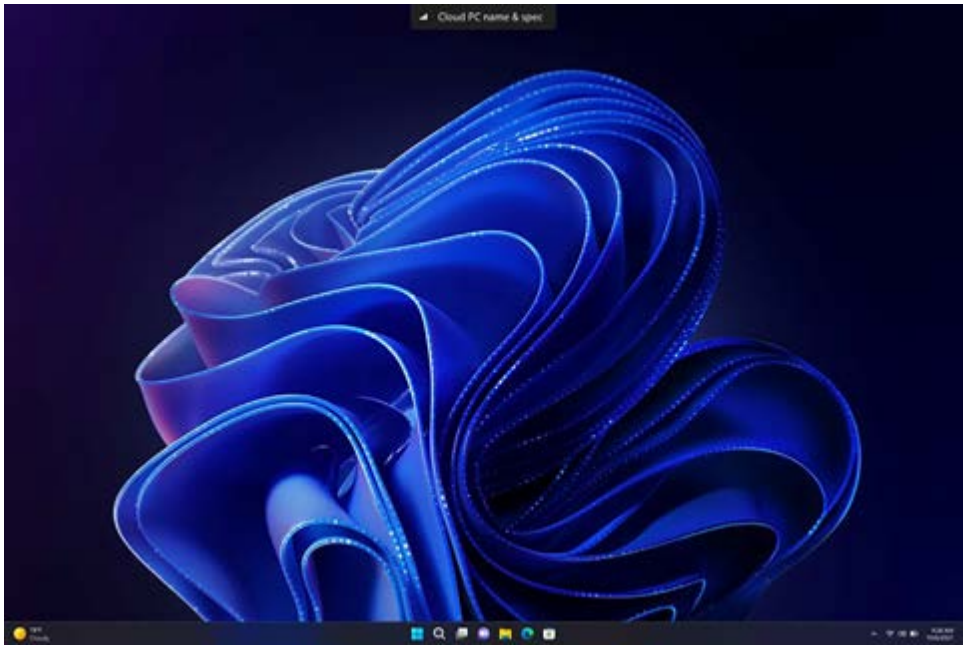


Figure 5.66: Cloud PC desktop

One of the new features of Windows 365 Boot shared mode is a customized company logo and name, which allows customization of the Windows Boot login page to include the company branding from Intune.

The feature will begin to be enabled for Windows 365 customers via a private preview in early 2024.

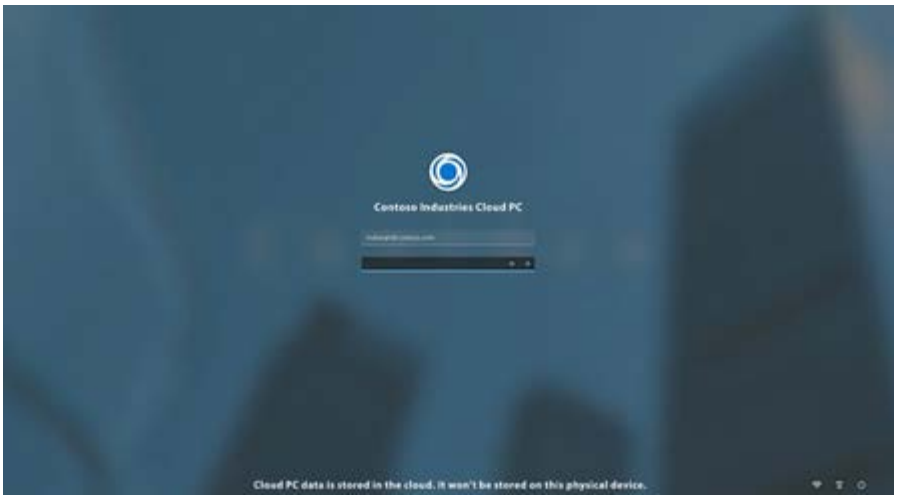


Figure 5.67: Windows 365 Boot shared mode is customized

17. You can enable the company logo and name branding in Microsoft Intune – you can find the changes under the **Settings** menu when deploying Windows 365 Boot shared mode.

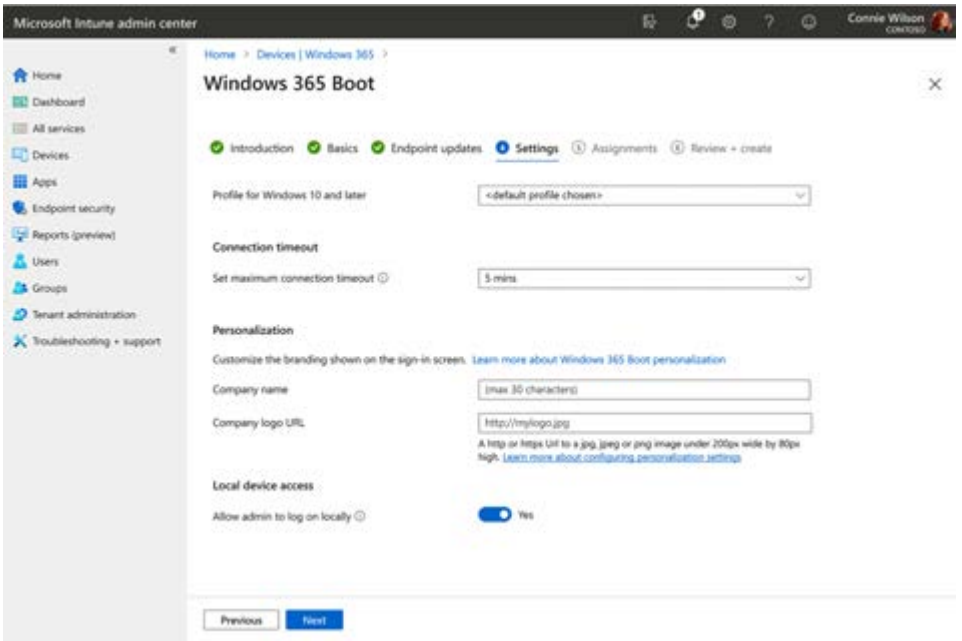


Figure 5.68: Windows 365 Boot

Another great improvement is our new fail-fast mechanism for Windows 365 Boot: You no longer need to wait for the sign-in process to the Cloud PC to complete only to find out Windows 365 Boot failed due to network issues or incomplete setup. The smart logic proactively informs users to resolve network issues or complete app setup so users can experience a smooth login to their Cloud PC.

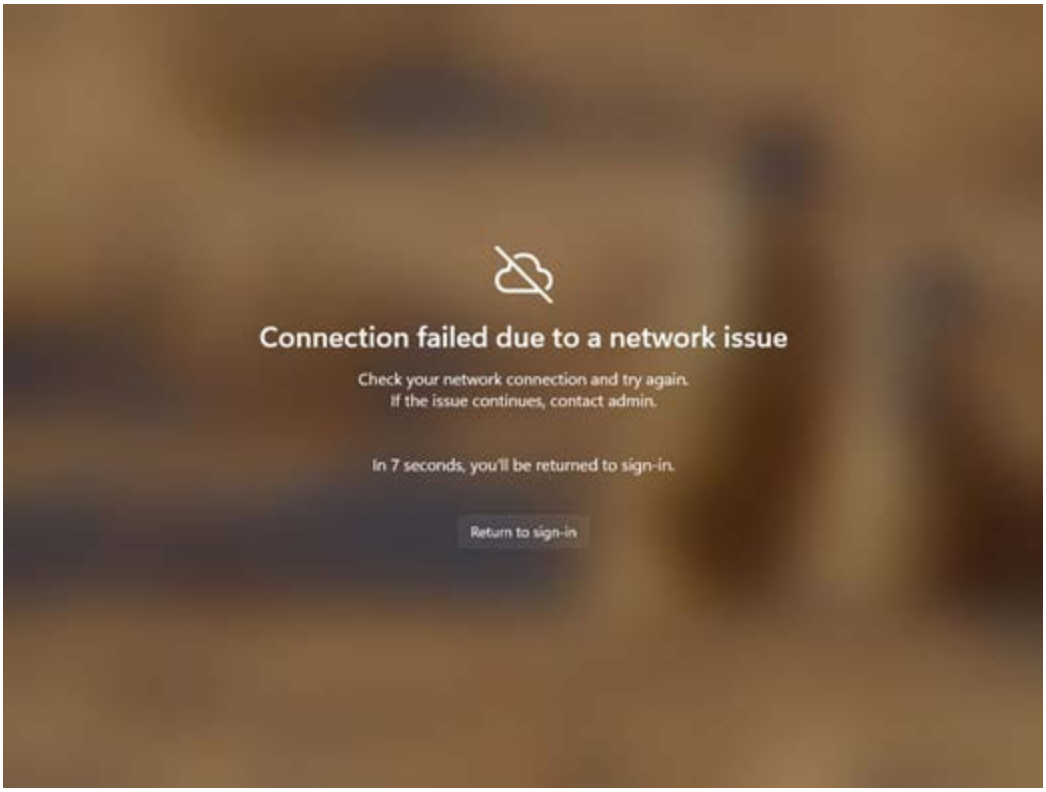


Figure 5.69: Connection failed

You can now also manage your local Windows 11 settings from within your Cloud PC. With this feature, it is now easier for you to access and manage sound, display, and other device-specific settings of your local PC directly from your Cloud PC in Windows 365 Boot.



Figure 5.70: Open local PC settings

Windows 365 Boot dedicated mode

You can now boot to your Windows 365 Cloud PC from your designated company-owned device. You will be able to seamlessly log in to your Windows 365 Cloud PC from the Windows 11 login screen using password-less authentication methods like Windows Hello for Business. Passwordless provides more seamless and frictionless logins and a reduced attack surface for credential stuffing, cracking, and phishing attacks.

In the previous section, you've seen how you can enable Dedicated User Mode via the new addon into our Windows 365 Boot-Intune guided flow scenario.

The new dedicated mode also comes with a fast account switcher experience to effortlessly switch profiles used during the login process, personalized experiences with your username and password, display picture on the lock and login screen, remember your username, and so on.

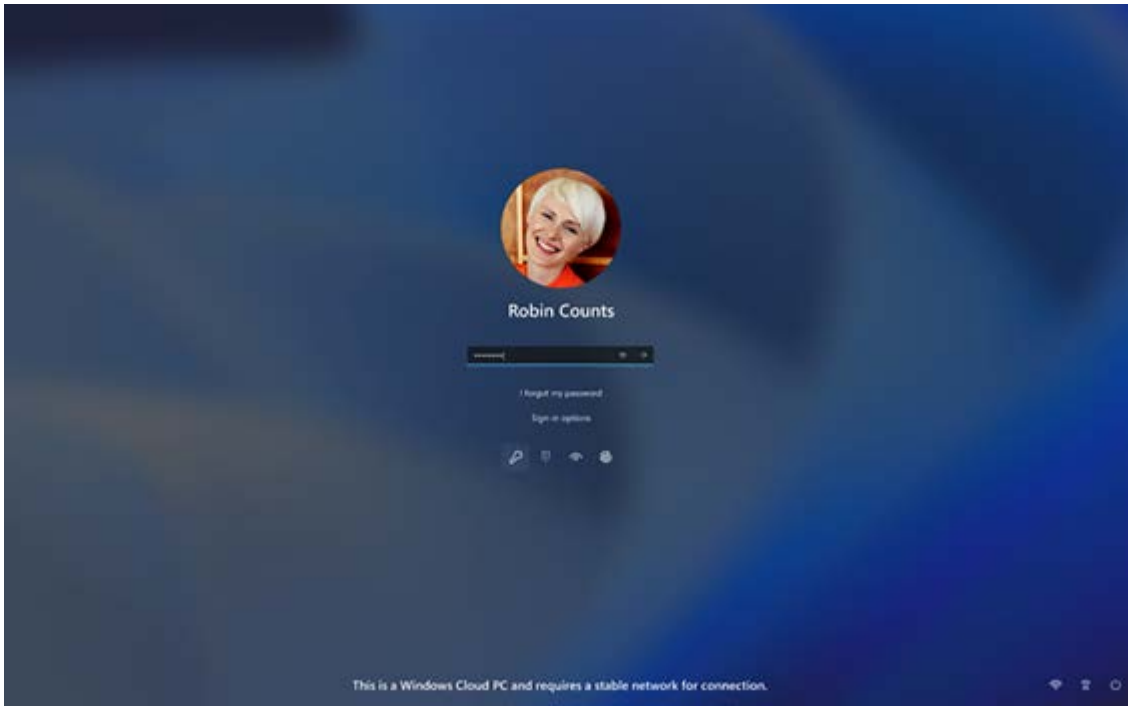


Figure 5.71: This is a Windows Cloud PC

What if you have multiple Cloud PCs?

End users have the power to handpick their Cloud PC of choice, making personalization a breeze via the Windows App client. Soon, users will be able to pick which Cloud PC they can use directly from the first logon experience, too!

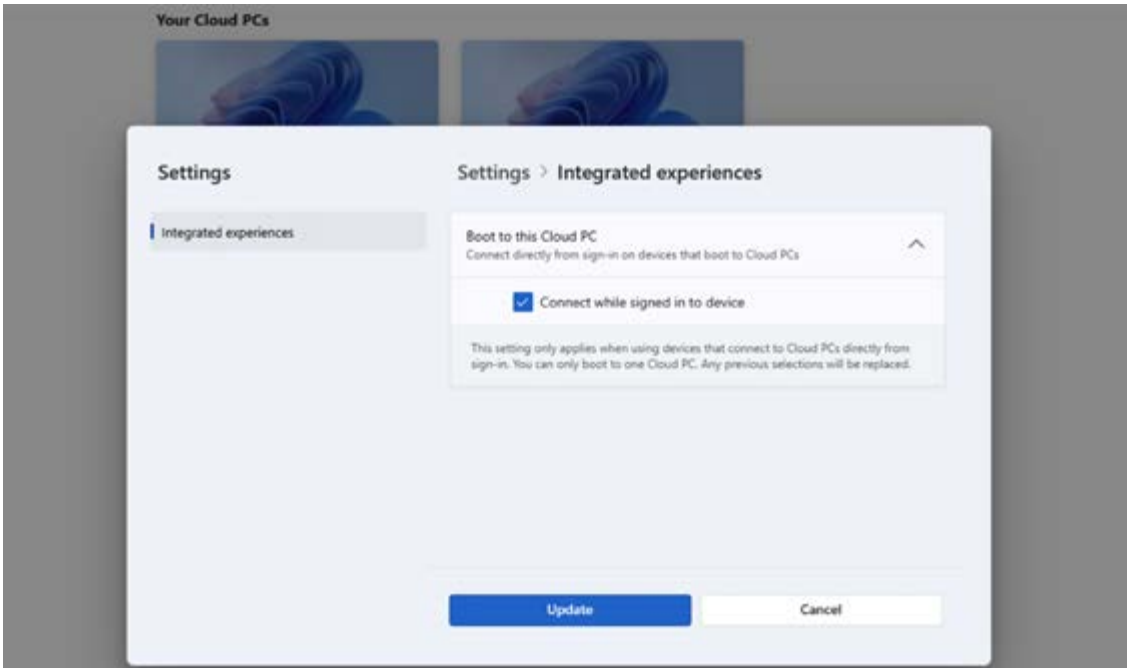


Figure 5.72: Integrated experiences

Battery status redirection

Windows 365 now also supports redirection of battery status information; for example, when using Windows 365 Boot dedicated mode on a surface laptop or another OEM device such as a Lenovo ThinkPad, you will be able to see how much battery you have left inside the Cloud PC session.

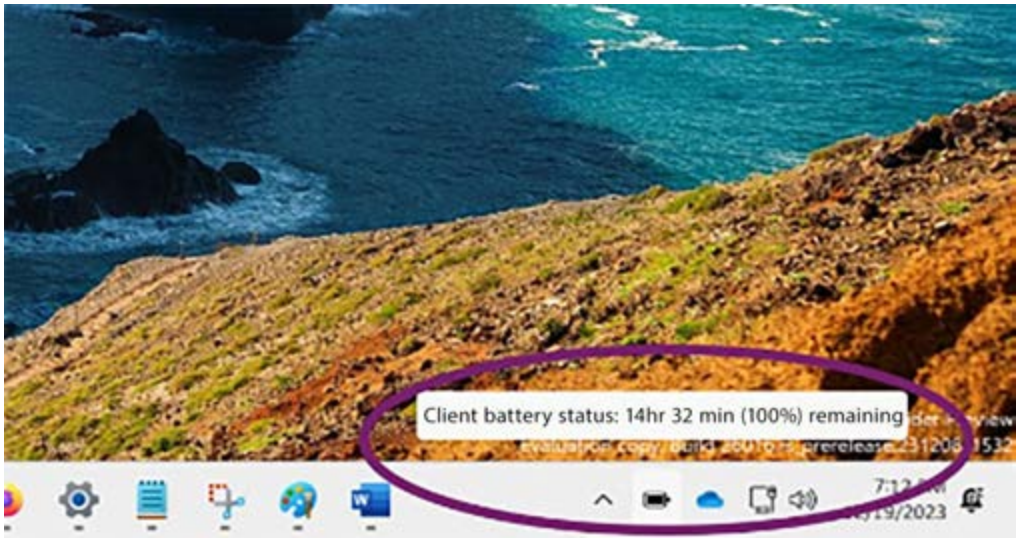


Figure 5.73: Battery status

Windows 365 Switch

Windows 365 Switch provides the ability to easily move between the Cloud PC and the local desktop using the same familiar keyboard commands *Alt* + *Tab*, as well as a mouse click or a swipe gesture. Everything works from within Windows 11 via the Task view feature. Windows App will be required on the endpoint and afterward, everything will show up automatically inside the Task view feature (see the following).

The hidden gem here is that users can do the same inside their Cloud PC, that is go to Task view and now switch back to the local PC.

This new round-tripping feature is extremely valuable for **bring-your-own-device** (**BYOD**) scenarios when you connect from your own Windows device to a secure company-owned Cloud PC. This is a great experience when businesses want to do more with less financial outlay.

Some of the most recent Windows 365 Switch improvements Microsoft has made are:

- **Improved disconnect experience for Windows 365 Switch:** You can now disconnect from your Cloud PC directly from your local PC. This can be done by going to the local PC and then the **Task** view, right-clicking on the **Cloud PC** button, and then selecting **Disconnect**.
- **Desktop indicators to differentiate between Cloud PC and Local PC for Windows 365 Switch:** You will now see the terms **Cloud PC** and **Local PC** on the desktop indicator when you switch between your respective PCs.
- **Gracefully handling increased connection time for Windows 365 Switch to Frontline Cloud PC:** You will now see updates regarding the Cloud PC connection status and the connection timeout indicator while waiting on the connection screen. If errors do occur, you can now copy the correlation ID using the new copy button on the error screen to aid with quicker resolution.



Note: The Task view can be found on the Windows Taskbar next to the **Search** button.



Figure 5.74: Windows Taskbar

Once you click on Connect to Windows 365, a similar Boot to Cloud PC experience will start as it did for Windows 365 Boot, however, now from a device that has Windows 11 completely available from the local PC.

During that connection process, you'll see the status displayed on the screen such as in the following figure.



Figure 5.75: Connection to your Cloud PC

Once you are inside the Cloud PC session, you can open the Task view feature from the Windows 11 Taskbar (next to **Search**) once more. In here, on the left side, you will find the **Local Desktops** option. Once you click on this, you will switch back to the local PC.

You can find more information about the Microsoft Taskview feature at `https://support.microsoft.com/en-us/windows/get-more-done-with-multitasking-in-windows-b4fa0333-98f8-ef43-e25c-06d4fb1d6960#WindowsVersion=Windows_11`.



Note: Once you establish the connection to the Cloud PC, switching to and from the Cloud PC will happen within less than a second!



Figure 5.76: Task view

Resize Cloud PCs

As an IT admin, you can upgrade Cloud PCs with more CPU, RAM, and storage. This means that the user can, for example, upgrade from a 2vCPU/4 GB RAM Cloud PC to a 2vCPU/8 GB RAM Cloud PC so that more resources are available for their workload.

Note that when you resize RAM, other options may also be changed, such as the storage (from 128 GB to 256 GB in the preceding example – as the higher SKUs do not all offer the same disk size options).

You can find this feature in the **Microsoft Intune** portal, under **Devices**, upon clicking the **Resize** button:

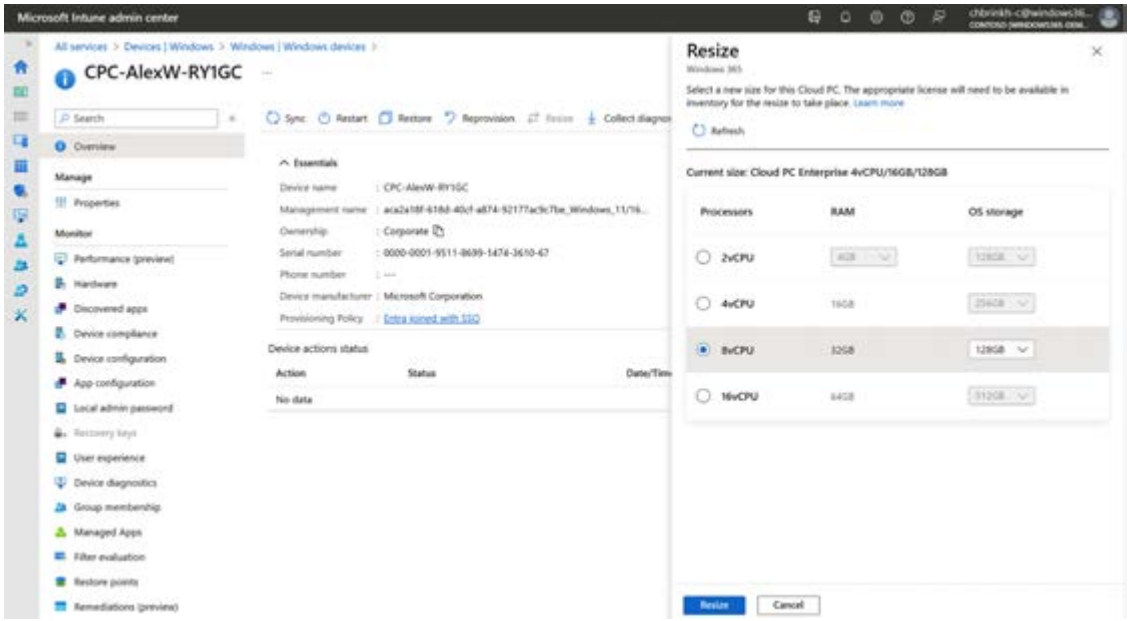


Figure 5.77: Resizing the Cloud PC feature

Bulk device actions

To manage your Windows 365 Cloud PC environment, you sometimes need to push configuration settings to multiple endpoints to provide actions at scale to a certain group of users.

Under **Devices** | **Windows**, you can find your endpoint objects to perform individual device actions, for example:

- Sync settings
- Restart the Cloud PC
- Restore to a previous point in time
- Reprovisioning the Cloud PC
- Resize
- Collect diagnostics
- Windows Defender settings (scan, update agent, etc.)
- Configure Remote Assistance
- Place the Cloud PC under review

1. Go to **All devices** in Intune, followed by **Bulk Device actions.**

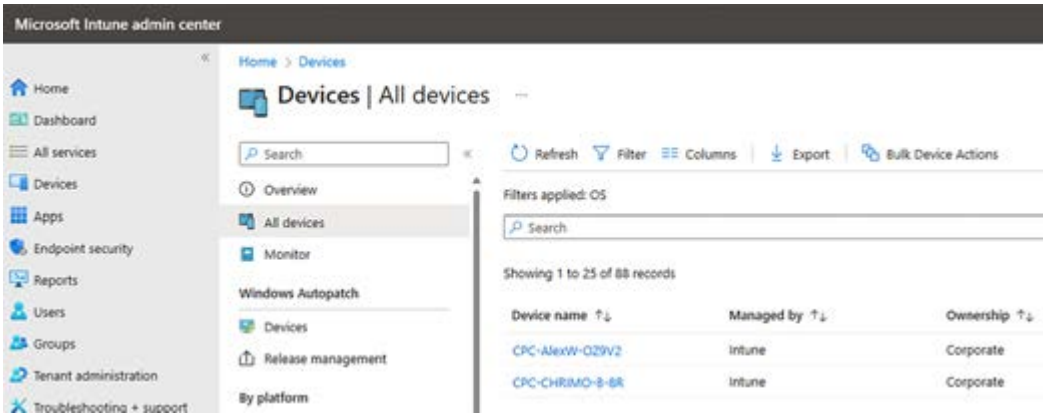


Figure 5.78: Bulk Device Actions

2. Select **OS Windows.**
3. Select **Cloud PCs** as **Device type.**
4. Select your bulk device action. Different variations are possible to make your life as an IT admin easier!

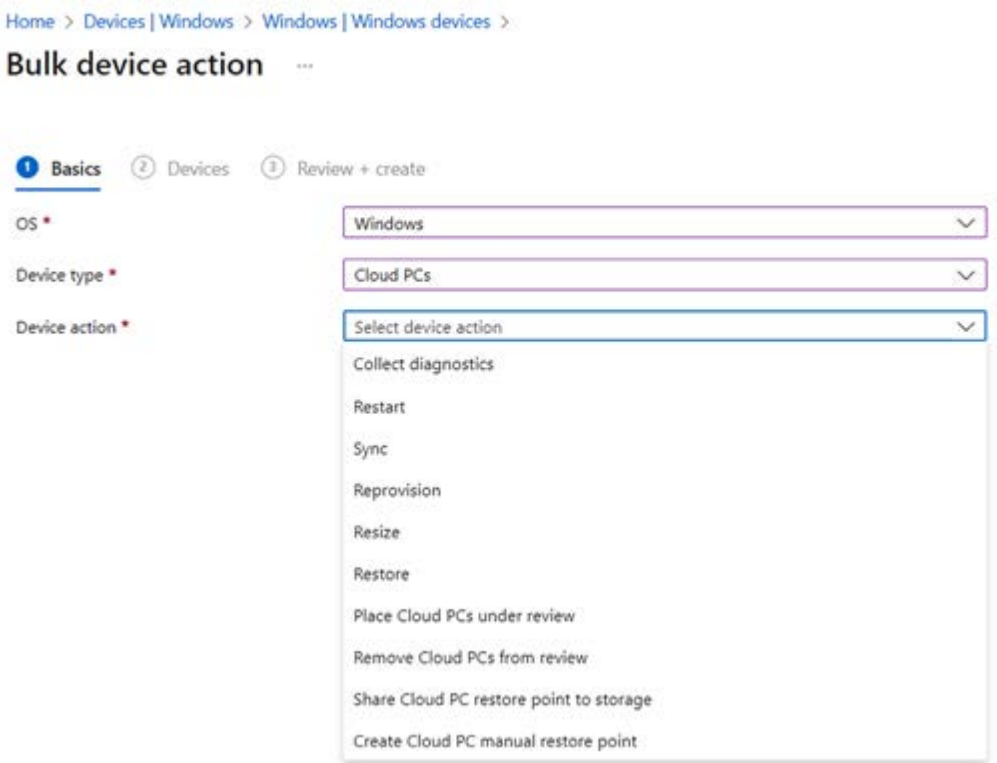


Figure 5.79: Bulk device action Cloud PCs

Monitoring and analytics

Ensuring that the performance and quality level of your Cloud PC environment is good is just as important as (or perhaps even more so than) the implementation. Users need to be happy about their Cloud PC and it should not impair their productivity.

Windows 365 Cloud PC seamlessly integrates with all the monitoring and analytics capabilities in Microsoft Intune that you use today for your physical endpoints. This means that you can easily distinguish whether the problem is active on the physical endpoint or within the Cloud PC session.

You will learn more about monitoring in *Chapter 14*, *Monitoring and Endpoint Analytics*, where we will take a much deeper dive into the specific metrics of ensuring the performance and quality of your Windows 365 environment both proactively and reactively!

Here's a quick preview list of the reports/dashboards that are available at the time of writing:

- Startup performance
- Proactive remediations
- Recommended software
- Application reliability
- Connectivity monitoring
- Resource performance
- Remoting connection

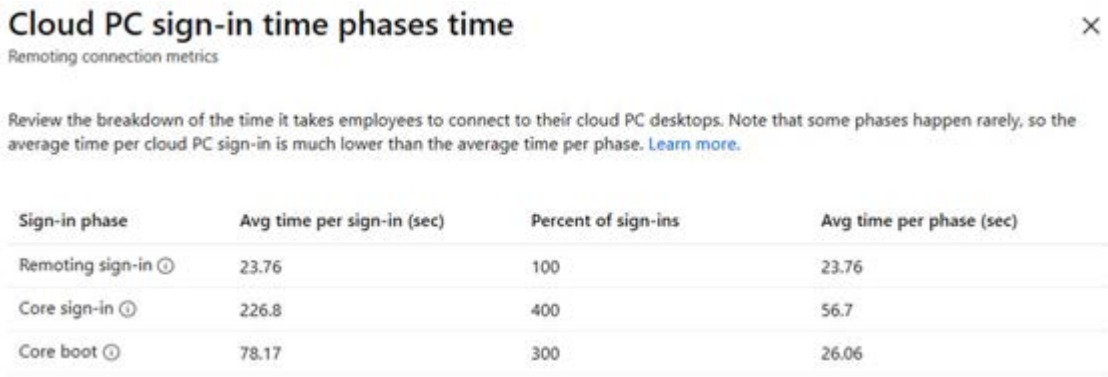


Figure 5.80: Sign-in time – logon duration, Endpoint Analytics



IMPORTANT NOTE

Endpoint Analytics and monitoring are provided as a free license with Windows 365 Cloud PCs. There are no consumption-based costs involved, so it's an easy way to calculate your costs next to your Microsoft fixed-pricing licensing model.

We also have a broad partner ecosystem that can help you with monitoring both physical and Cloud PCs, such as ControlUp Enrich. Learn more about it via `https://microsoftedge.microsoft.com/addons/detail/controlup-enrich/jpnanfoohdfeigkhpljklbgccfbccafp`.

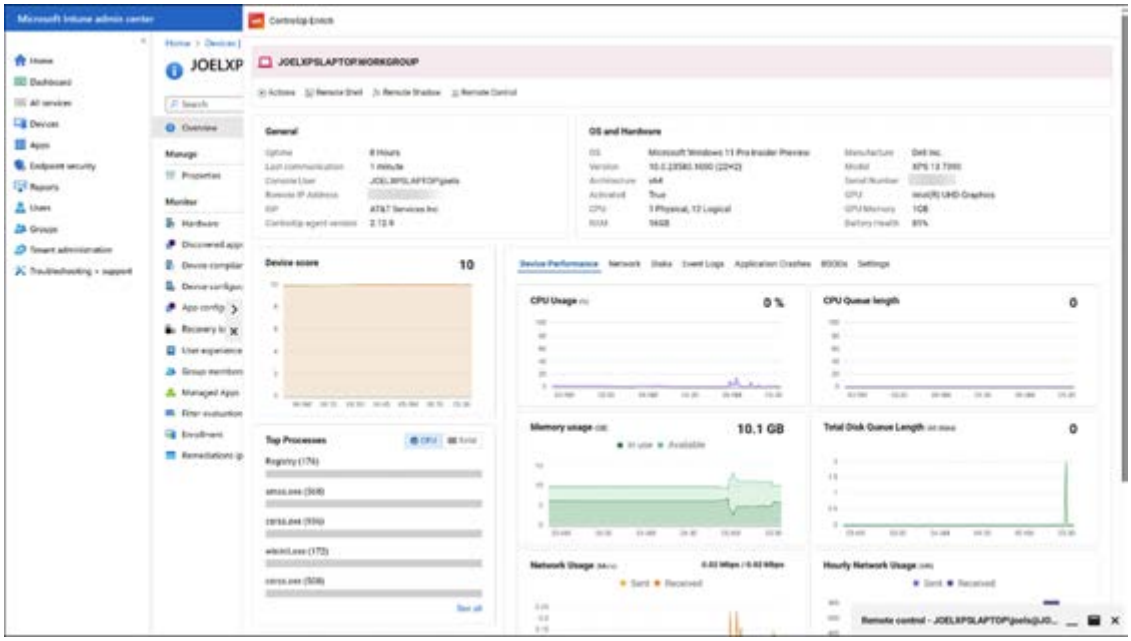


Fig 5.81: ControlUp Enrich

Now, we briefly touched on how AI can help you resize; let's explain how you can use the Intune Suite together with Windows 365 Cloud PCs.

Intune Suite – Endpoint Privilege Management

Avoiding providing local administrator rights should always be the primary goal when configuring permissions for users. With the new Intune Suite and Windows 365 integration, we make it possible to start applications with extra privileges. Note that the features within the Intune Suite incur extra licensing costs.

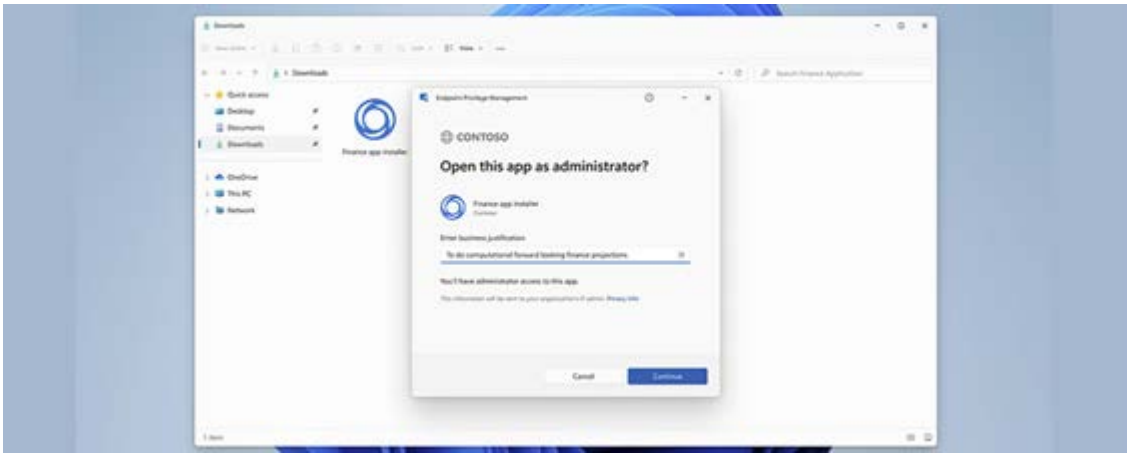


Figure 5.82: Windows 365 Endpoint Privilege Management

Intune Suite – Enterprise App Management

With Enterprise App Management, you can simplify and unify the application update process, both for first- and third-party applications! You can see all the apps that need an update on a single, user-friendly screen. You can also compare the current and new versions of the apps in the catalog. You can save time and effort by avoiding the manual work of tracking updates and collecting application-related data and packaging. You can focus on more important tasks as an admin.

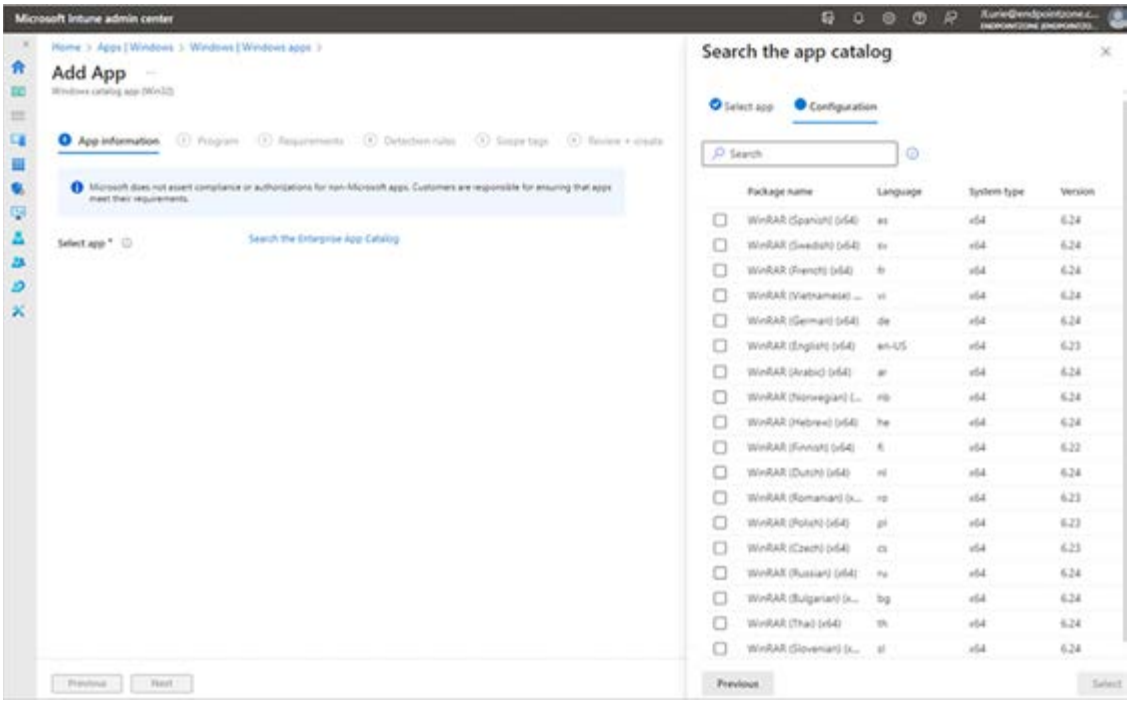


Figure 5.83: Windows 365 Enterprise App Management

Intune Suite – Remote Help

Remote Help is a cloud-based solution that allows secure connections between help desk staff and users' devices. The staff can access the devices remotely with different levels of permissions. During the session, the staff can see the device's screen and, with the user's consent, take full control. Full control lets the staff make changes or perform tasks on the device directly.

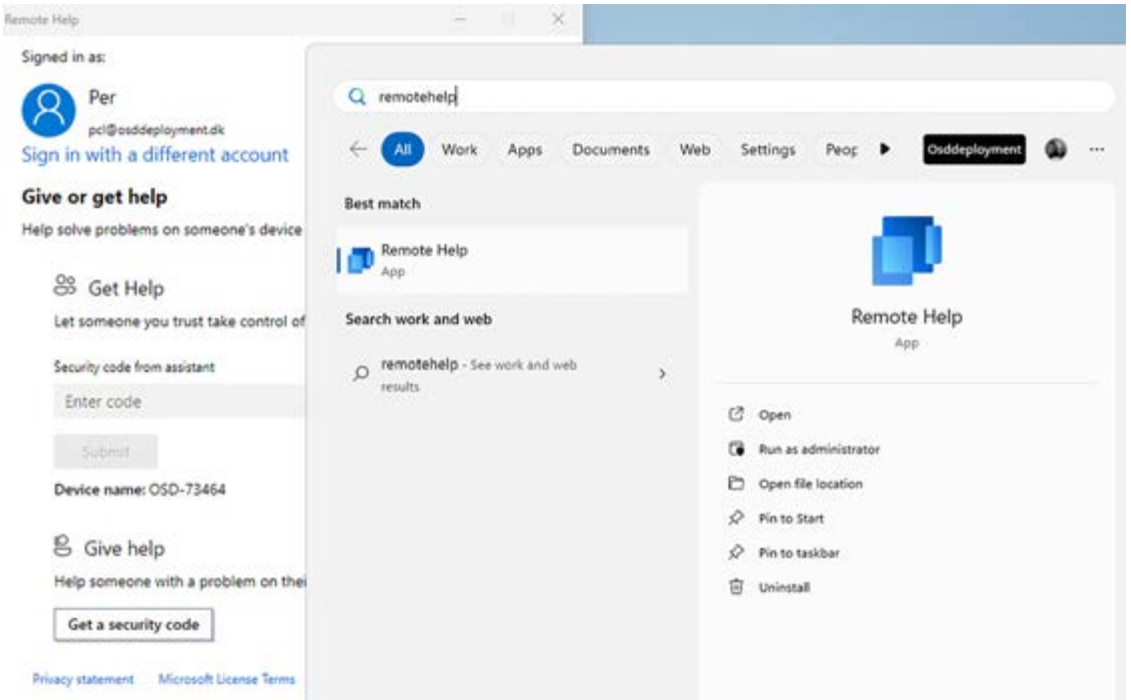


Figure 5.84: Windows 365 remote Remote Help

You will learn more about Intune Suite in Intune Suite *Chapter 11*, where we take a deep dive into its features.

Want to dive deeper into Windows 365?

If you want to go even deeper into Windows 365, we recommend you purchase the book **Mastering Windows 365**, released by Christiaan Brinkhoff, Sandeep Patnaik, and Morten Pedholt.

This level 500+ technical deep dive goes further into details of the RDP protocol and other tips and tricks. The book is a great add-on to this book, and will look amazing on your bookshelf! You can purchase the book via Amazon, Packt, or directly via `aka.ms/MasteringW365`.

With that, we have come to the end of this chapter. Congratulations on completing it!

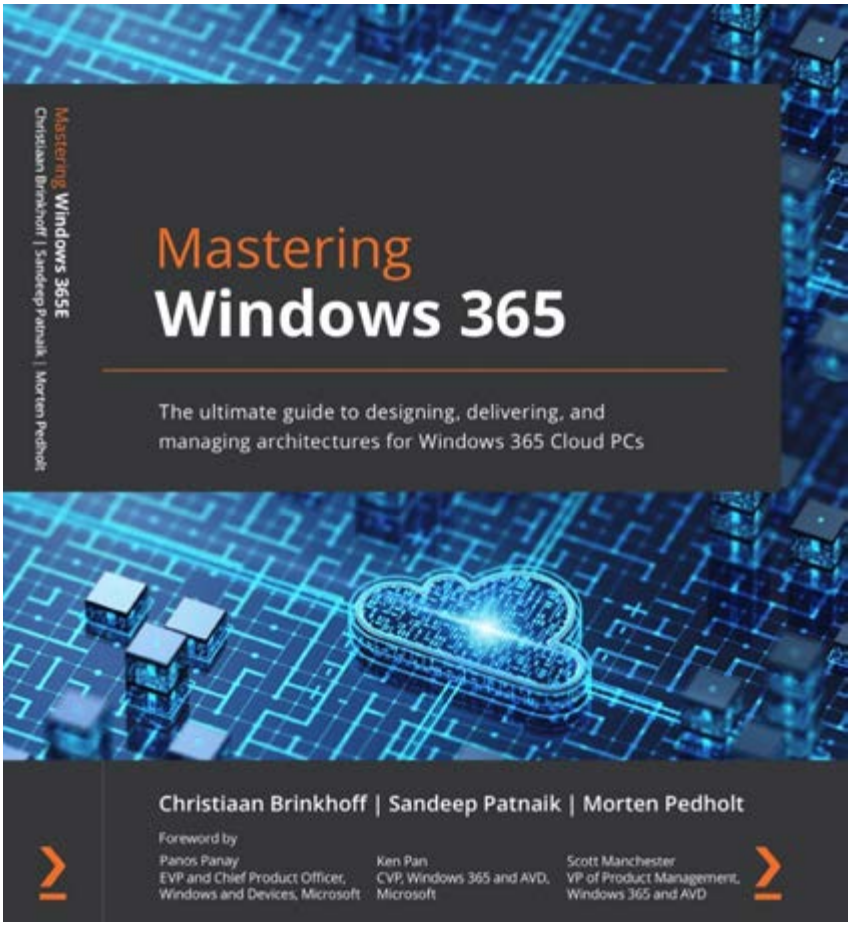


Figure 5.85: Mastering Windows 365

Summary

In this chapter, you've learned everything you need to know about the new Windows 365 service, from the fundamentals of it to deep diving into the logistics of configuration. We covered all the steps required to deploy Windows 365 Enterprise, what the prerequisites are, and some other great tips to learn more about different optimizations for your deployment.

In the next chapter, we will take a deeper dive into the different aspects of managing your Windows 365 environment, as well as thinking about monitoring, application distributions for classic Windows applications (Win32) and MSIX, identity and security, and many more aspects.

Questions

1. Can you move existing Cloud PCs to other regions without losing any user and application data?
    a. Yes
    b. No
2. What protocol is Windows 365 using as part of connecting to Cloud PCs?
    a. Unified Desktop Protocol
    b. Blaster Disaster Protocol
    c. Remote Desktop Protocol

Answers

1. a
2. c

Further reading

If you want to learn more about Windows 365 after reading this chapter, please go to one of the following other sections in this book:

- *Chapter 12*, *Copilot/AI*
- *Chapter 13*, *Identity and Security Management*
- *Chapter 14*, *Monitoring and Endpoint Analytics*
- *Chapter 16*, *Troubleshooting Microsoft Intune*

Get This Book's PDF Version and Exclusive Extras

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

Note: *Keep your invoice handy. Purchases made directly from Packt don't require one.*

UNLOCK NOW

Section III

Mastering Microsoft Intune

This section explains everything you should know about the configuration and management process for Microsoft Intune as well as other services that you can use to modernize your existing Windows Enterprise deployment. After reading this section, you will have enough knowledge to start deploying.

This part of the book comprises the following chapters:

- *Chapter 6*, *Windows Deployment and Management*
- *Chapter 7*, *Windows Autopilot*
- *Chapter 8*, *Application Management and Delivery*
- *Chapter 9*, *Understanding Policy Management*
- *Chapter 10*, *Advanced Policy Management*
- *Chapter 11*, *Intune Suite*
- *Chapter 12*, *Copilot/AI*
- *Chapter 13*, *Identity and Security Management*
- *Chapter 14*, *Monitoring and Endpoint Analytics*
- *Chapter 15*, *Universal Print*

6

Windows Deployment and Management

In this chapter, you will get a clear understanding of how to deploy and update Windows in enterprises with Microsoft Intune and Windows Update for Business. You'll learn about the different deployment methodologies and other features that you can use to provide Windows updates and management at the enterprise level, such as with Windows Autopatch!.

In this chapter, we'll go through the following topics:

- Deploying existing Windows devices into Microsoft Intune
- What about on-premises devices?
- Co-management
- Tenant attach
- Microsoft Surface and other **Original Equipment Manufacturer** (**OEM**) devices
- **Windows Update for Business** (**WUFB**)
- Windows 10 and Windows 11 update rings
- Windows Autopatch
    - Windows Autopatch requirements
    - How to enable Windows Autopatch
    - Optimize Windows Update Rings
    - Enable Autopatch for Cloud PCs

Deploying existing Windows devices into Microsoft Intune

This scenario applies to physical Windows endpoints only.

In enterprise companies today, the normal approach is to leverage OS deployment either from Configuration Manager or Microsoft Deployment Toolkit.

Microsoft Deployment Toolkit (**MDT**) is simpler as it only requires access to a share, where the Windows 10 OS drivers and applications are stored. Microsoft does not support MDT Windows 11 OS deployment.

Both Configuration Manager and MDT often require the device to be on-premises to join the corporate **Active Directory** (**AD**) and have access to the **Preboot Execution Environment** (**PXE**) server to even get started with OS deployment.

Over the last few decades, enterprise companies have started to remove all the work that the OEM put into making a device run in the most optimal way with Windows 10, drivers, and the combination of settings that are needed on a brand-new device to perform in the best way possible. This was done by leveraging a *wipe-and-load* imaging concept, and only what the company approved to be installed on the devices would be installed. Normally, this would be an older version of Windows, older versions of drivers, and Microsoft Enterprise apps.

If only it were possible to do this in a simpler way and from anywhere. With the outbreak of COVID-19 and with almost everybody working from home, luckily, modern technology has allowed us to disconnect from physical locations and move to working from anywhere. This also includes provisioning a brand-new device to an end user's home address without the end user needing to go to the office location and get the new device. This is possible today with a modern provisioning solution called Windows Autopilot. The benefit of using Windows Autopilot is that provisioning can be done from anywhere as long as there is internet connectivity. The process is simpler and takes the complexity out of provisioning a brand-new device. We will cover Windows Autopilot at a high level in this chapter, and then in more depth and with real-life examples in the next chapter.

Windows Autopilot is a group of different components of technology that come together into one service to configure new devices out of the box to get them ready for production usage. The cool thing about Autopilot is that you can also use it to reset, repurpose, and recover devices from scratch if you want to start over again. This is all done to release the IT department from doing all this work themselves; there's no infrastructure to manage as Autopilot runs as a cloud service within Microsoft Intune, so it's much easier and faster to get productive!

In a break-and-fix scenario where the hard drive is changed, we highly recommend having an agreement with your OEM to provide a new hard drive with Windows on it ready to go through the **Out of Box Experience** (**OOBE**), or leverage the OEM's cloud recovery options. If that is not possible, Microsoft provides several options to get the OS onto the device, including a media creation tool for Windows 11 that can be downloaded from here: `https://www.microsoft.com/en-us/software-download/windows11`.

Enrolling devices – Windows enrollment

In this section, we will learn several different ways that Windows 10 or Windows 11 PCs can be enrolled in Intune by users or admins. The IT admin can configure Windows device enrollment under **Devices** | **Enroll devices** | **Windows enrollment** inside the admin center portal. We will cover the different options later in the book. The best option for end users is to enroll through Windows Autopilot for corporate-owned devices.

For BYOD, the end user can enroll in Intune in a number of different ways. One is to download Company Portal from the Windows Store and sign in and onboard that way. Another option is provided in the **Windows Settings** app under **Accounts** and then **Access work or school.**



IMPORTANT NOTE

Windows 365 Cloud PCs are automatically enrolled in Microsoft Intune.

Automatic enrollment

This section covers configuring Windows devices to enroll when they join or register **Microsoft Entra ID (Entra ID)**. We covered this in a previous chapter, *Chapter 3*, *Requirements for Microsoft Intune*, so please go back to that chapter to learn more.

Your starting point for Windows enrollment is shown here:

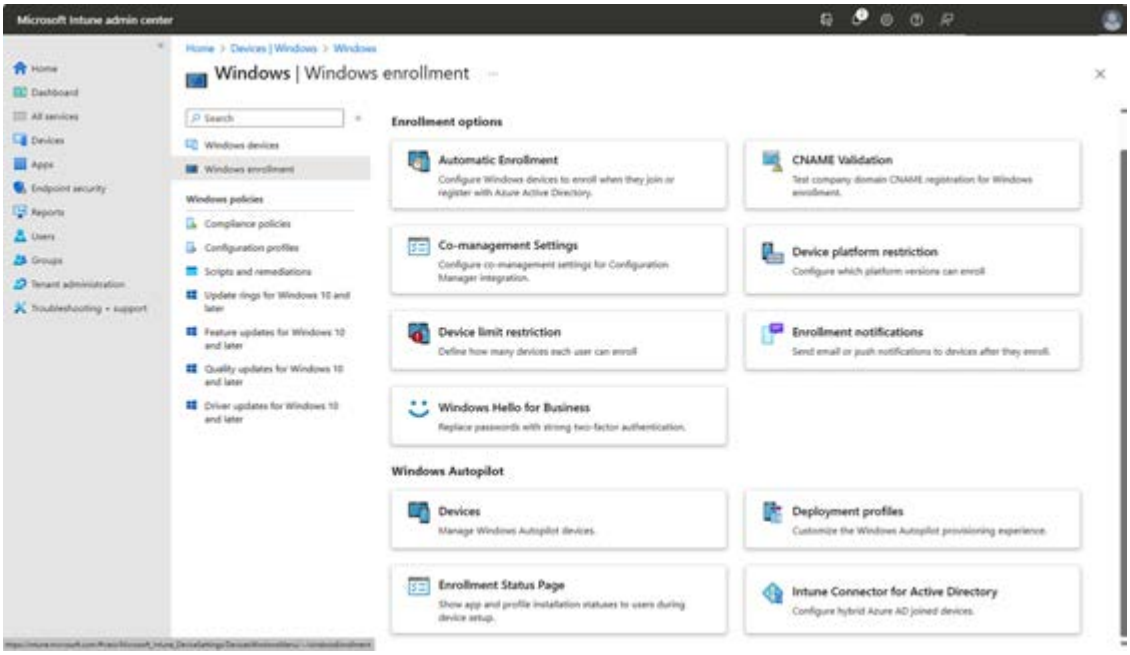


Figure 6.1: Windows enrollment

Testing company domain CNAME registration for Windows enrollment

Configuring a CNAME in your DNS saves your users from having to enter the address of the **Mobile Device Management** (**MDM**) server when enrolling their Windows devices. This means that the IT admin can enable auto-discovery of the Intune enrollment server.

The entries you need to create are the following:

Type	Host name	Points to	TTL
CNAME	`EnterpriseEnrollment.osddeployment.dk`	`EnterpriseEnrollment-s.manage.microsoft.com`	One hour
CNAME	`EnterpriseEnrollment.us.osddeployment.dk`	`EnterpriseEnrollment-s.manage.microsoft.com`	One hour
CNAME	`EnterpriseEnrollment.eu.osddeployment.dk`	`EnterpriseEnrollment-s.manage.microsoft.com`	One hour

Here, `osddeployment.dk` should be your company UPN. If you have several UPNs, you need to create DNS records for each of them.

After configuring the CNAME resource records in your DNS, enter the corresponding domain to confirm that it has been configured correctly.

Changes to DNS records might take up to 72 hours to propagate. You can find the configuration option that makes this possible in the following screenshot:

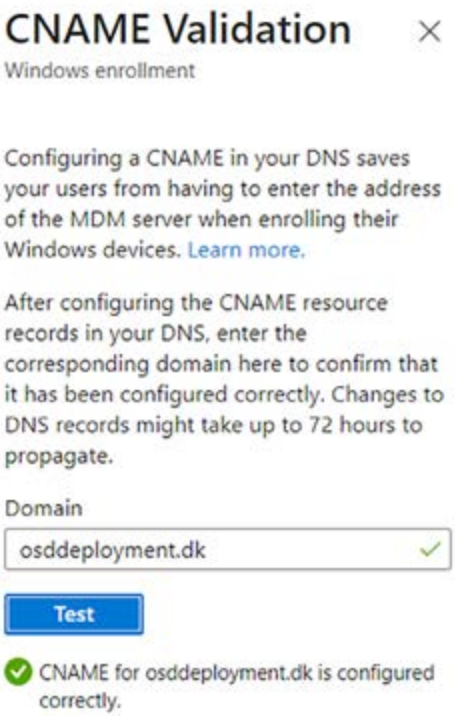


Figure 6.2: CNAME validation setup

Let's now switch over to the **Enrollment Status Page** screen to learn more about the results and status of your enrollment into Microsoft Intune.

Enrollment Status Page

The **Enrollment Status Page** screen displays the provisioning progress on Windows devices after a new device is enrolled, as well as when new users sign in to the device. This feature allows IT administrators to choose whether to restrict access to the device until the provisioning process is complete, while, at the same time, giving users information about the tasks remaining in the provisioning process.

In the **Enrollment Status Page** section in the Intune portal, the default **Enrollment Status Page** applies to all users and all devices, but you can create multiple Enrollment Status Page profiles with different configurations and priorities as required for your different scenarios. Those scenarios could be for shared PC's, Kiosk's, etc. where you need to have different configurations in the Enrollment Status Page.

These profiles are specified in priority order; the highest priority that is applicable will be used (the default **Enrollment Status Page** (**ESP**) will be the lowest priority). Each Enrollment Status Page profile can be targeted at groups containing devices or users. When determining which profile to use, the following criteria will be followed:

- The highest-priority profile targeted at the device will be used first.
- If there are no profiles targeted at the device, the highest-priority profile targeted to the current user will be used. (This only applies in scenarios where there is a user. In white-glove and self-deploying scenarios, only device targeting can be used.)
- If there are no profiles targeted to specific groups, then the default Enrollment Status Page profile will be used.

The **Enrollment Status Page** is not just applicable to Windows Autopilot devices but to all Windows devices that are enrolled in Microsoft Intune that have it assigned either to users or devices.

We will cover Windows Autopilot in depth, including how to set it up and configure the Enrollment Status Page for different scenarios, in the next chapter.

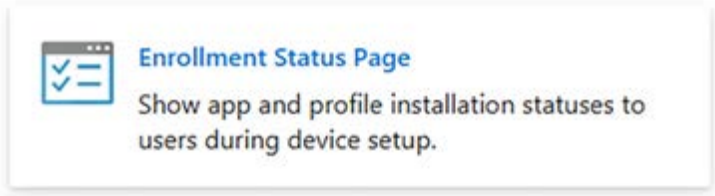


Figure 6.3: Enrollment Status Page

In the following screenshot, you can see multiple ESP profiles on the **Enrollment Status Page** screen:

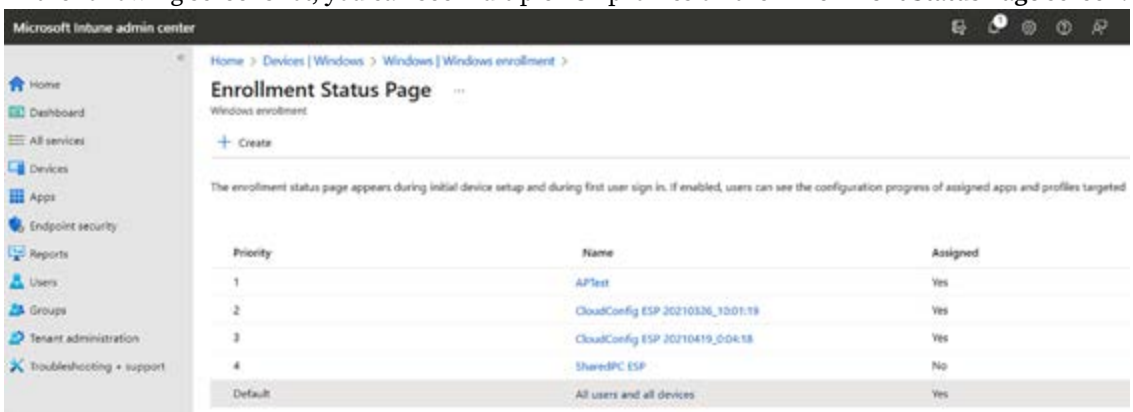


Figure 6.4: Enrollment Status Page screen

This concludes the section on the **Enrollment Status Page.** In the next section, we will cover enrollment notifications.

Enrollment notifications

Enrollment notifications in Microsoft Intune are used to notify employees of newly enrolled devices. This is a way for the end user to take action if the new devices were not enrolled by them. These notifications are sent to assigned users via email or push notifications and can be customized with a custom message, branding, and device details.

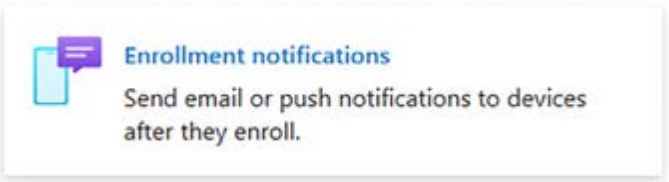


Figure 6.5: Enrollment notifications

Enrollment notifications are supported on multiple platforms in Intune, including Windows 10/11.

Enrollment notifications require that there is an end user that enrolls the device, so only user-driven scenarios are supported for Windows devices. It also means that userless scenarios such as Windows Autopilot for pre-provisioned deployments do not support enrollment notifications. Hybrid Entra joined devices are not supported.

To start creating enrollment notifications for Windows, follow these steps:

1. Go to **Devices** | **Windows** | **Windows enrollment** | **Enrollment nofications**.
2. Click **Create notifications**.

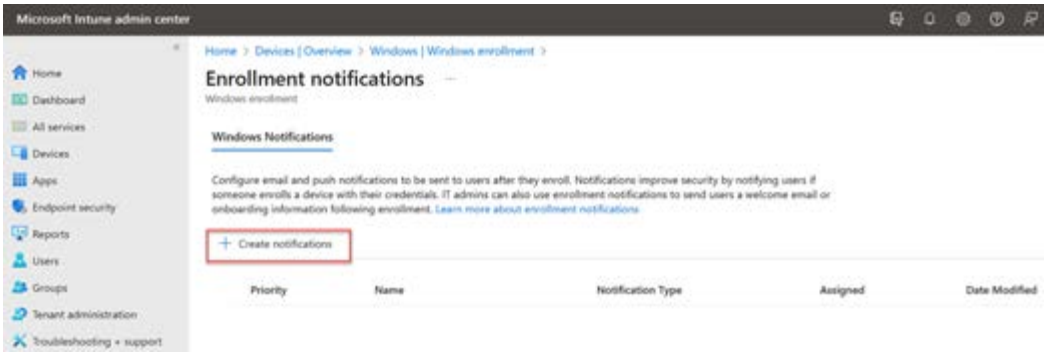


Figure 6.6: Enrollment notifications policy creation

In this example, we will create an enrollment notification and assign it to all users.

3. Enter `Enrollment Notifications Company enrollment` into the **Name** field.

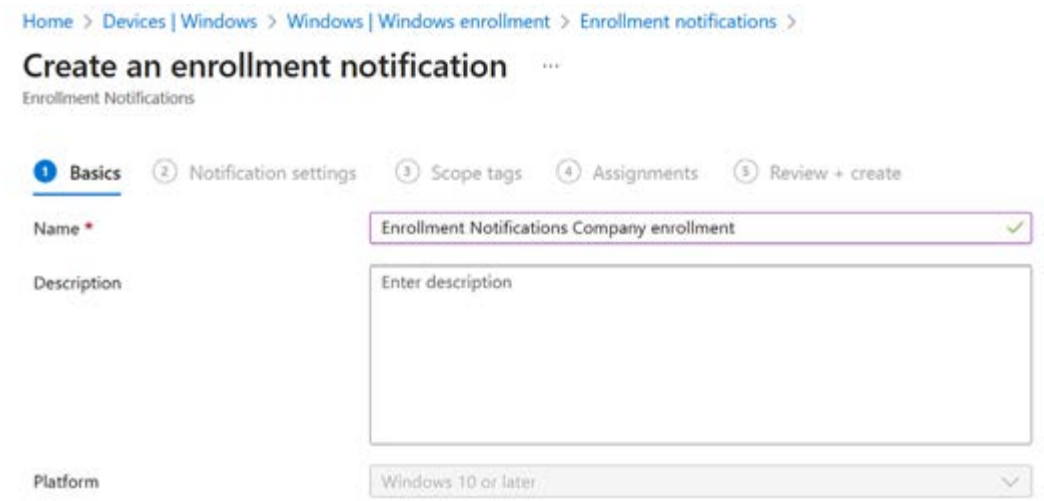


Figure 6.7: Enrollment notification name creation

4. Push notifications show up in Company Portal and are only supported on iOS/iPadOS, macOS, and Android, meaning that push notifications will never appear on Windows devices.
5. Enable email notifications by setting **Send Email Notification** to **On**.

6. Enter your message for the end user in HTML format (there is a 2,000-character limit), as shown in the image below.

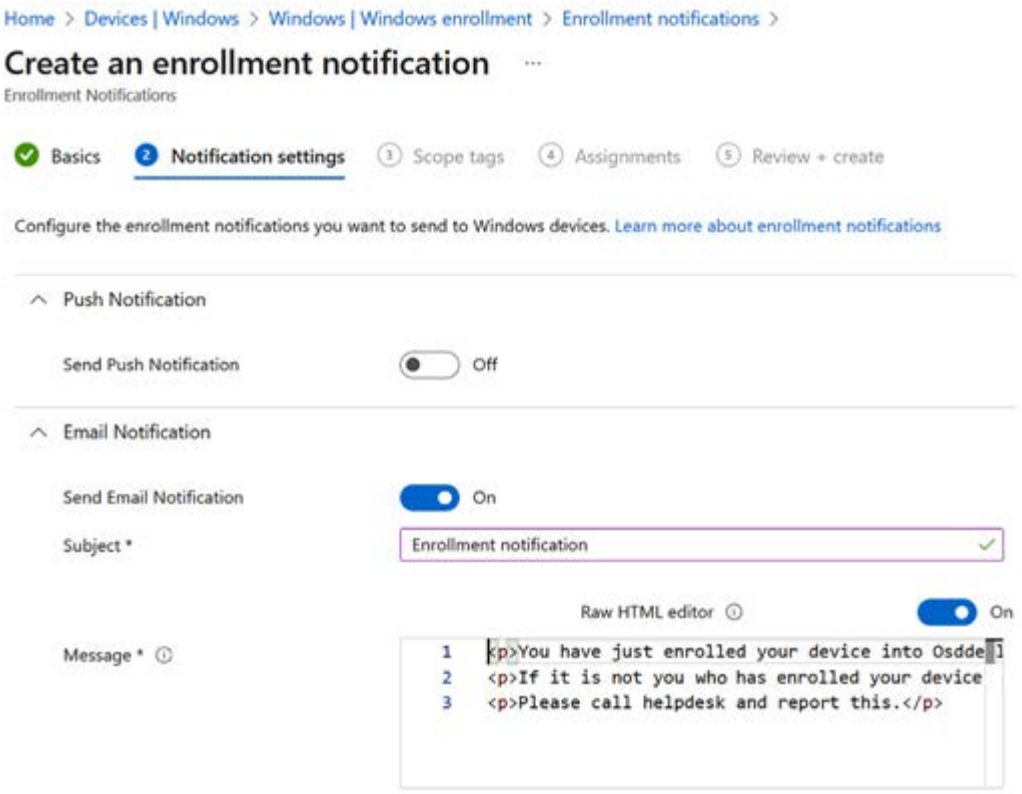


Figure 6.8: Enrollment notification policy part #1

You can use the built-in raw HTML editor to format and style email notifications.

Intune supports the following HTML tags: `<a>`, `<strong>`, `<b>`, `<u>`, `<ol>`, `<ul>`, `<li>`, `<p>`, `<br>`, `<code>`, `<table>`, `<tbody>`, `<tr>`, `<td>`, `<thead>`, and `<th>`. It also supports the **href** attribute for hyperlinks, but only for HTTPS links.

7. Enable **Email header** and **Email footer** to give the email notifications the company's default look and feel using the logo and company name from the Company Portal branding.

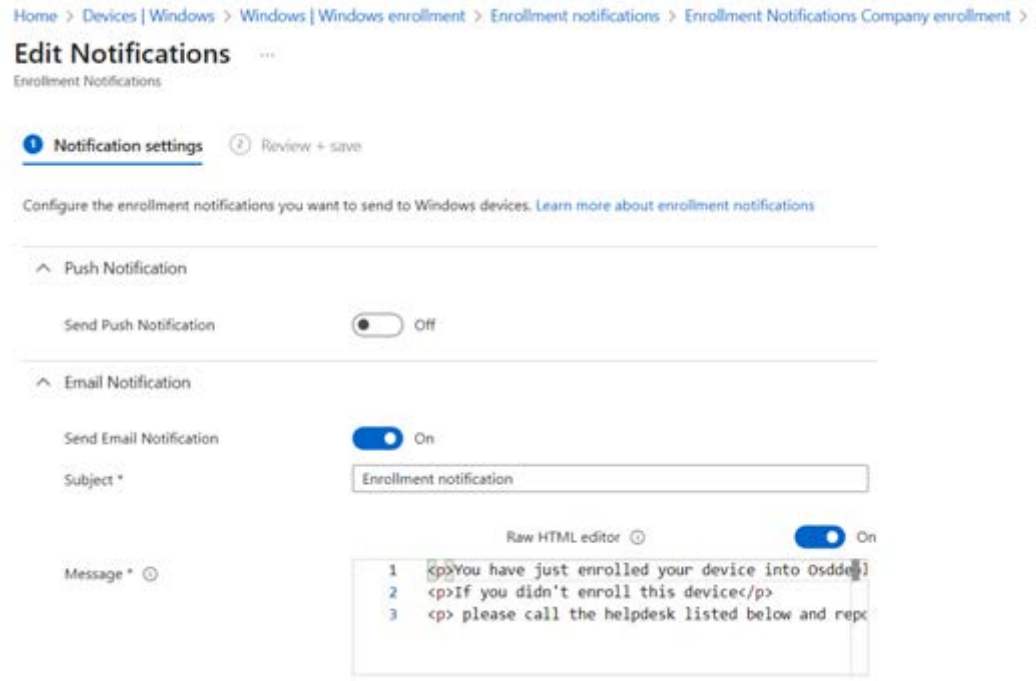


Figure 6.9: Enrollment notification policy part #2

8. Contact information in the email notifications also comes from the Company Portal branding, and cannot be changed when configuring the enrolment notification, only enabled or disabled.
9. Enabling the **Show company portal website link** option in the email notification profile guides the end user directly to the enrolled device in the Company Portal website when they receive the enrollment notification email.

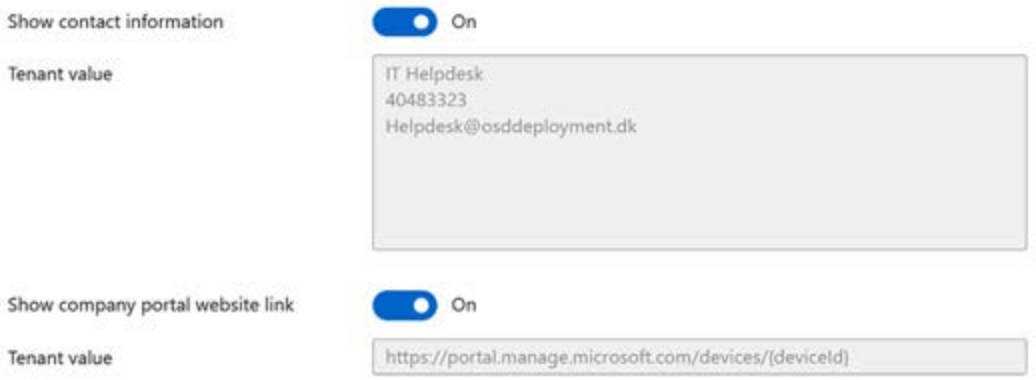


Figure 6.10: Enrollment notification policy part #3

10. Assign the email notifications to all users, and the next time one of your users enrolls a Windows device in Intune, they will receive an email that looks like this:



Figure 6.11: Enrollment notification email

11. If you click **View details**, it will open a browser with the web version of Company Portal:

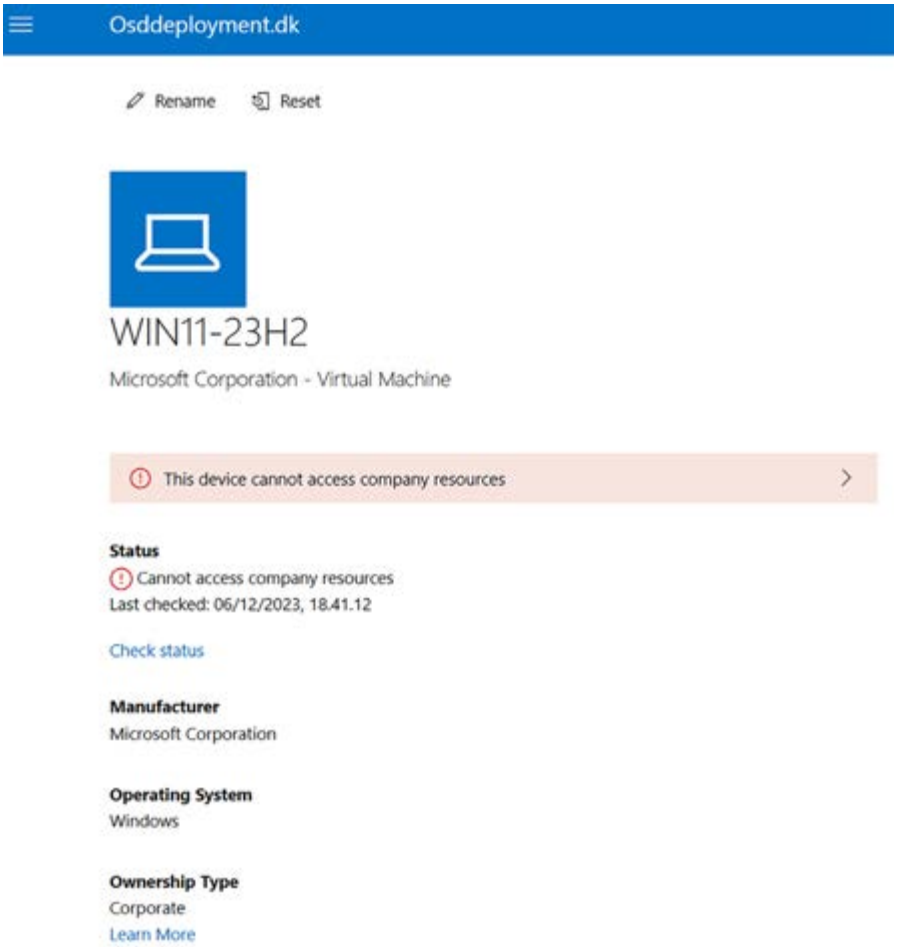


Figure 6.12: Enrollment notification email details view

As you can see, this device is not complaint. We will cover compliance policies and how to configure and troubleshoot them in *Chapter 10*.

Windows Autopilot

In this section, you will learn a bit more about Autopilot. We will spend a lot of time on Autopilot in *Chapter 7*, *Windows Autopilot*, later in the book.

Windows Autopilot works with deployment profiles that let you customize the OOBE for your devices – you need to have a separate Autopilot deployment profile for each scenario you will cover. This makes it easier for customers to create their own sets of configuration items out of the box without any user interaction. We'll explain more about this in the next chapter.

Windows Autopilot is built to simplify the Windows device life cycle, for both IT teams and end users, from initial deployment to end of life. Using cloud-based services, Windows Autopilot does the following:

- Reduces the time IT spends deploying and managing devices
- Reduces the infrastructure required to onboard and maintain devices
- Has the option for end users and IT admins to use break-fix or Autopilot Reset

More information about the Autopilot enrollment flow can be gathered from the following diagram, based on the profiles explained earlier in this section:

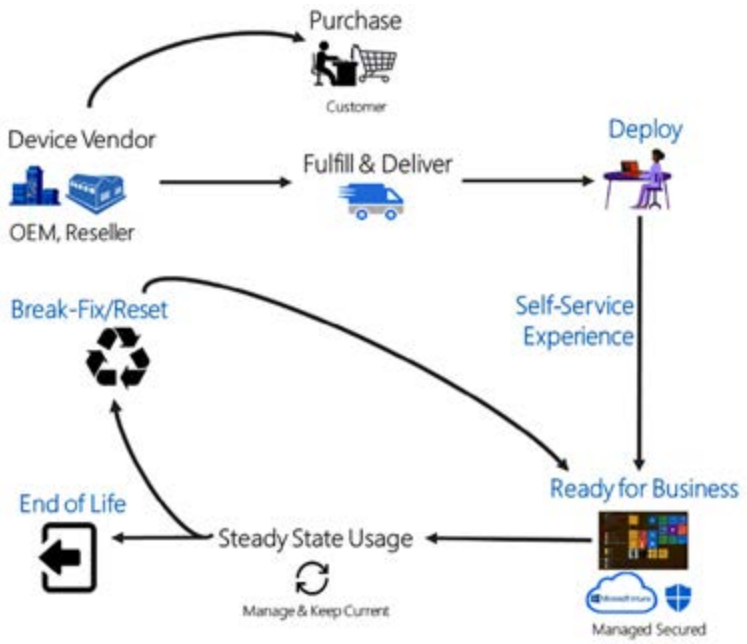


Figure 6.13: Autopilot process

Once you have deployed Windows Autopilot, it is important that your organization keeps up to date with the latest Windows releases. Many companies refer to this as *being evergreen*. To help your organization stay current, you should look into Windows Update for Business, which you have to configure and manage, or use Windows Autopatch, which is offered as a managed service from Microsoft, where you, as an IT admin, just need to monitor your updates.

Windows Autopilot supports both Entra ID joined and Hybrid Entra ID. The recommendation when starting to leverage Windows Autopilot in your organization is to use Entra ID as it is way less complex, and does not have the same requirements as Windows Autopilot for Hybrid Entra ID. With Windows Autopilot for Hybrid Entra ID, it can take a very long time (up to 40 minutes or sometimes even more) for a device to be hybrid joined and the device subsequently gets stuck in the ESP.

Hybrid Windows Autopilot also requires a line of sight to your domain controller, that can be done from anywhere via a connection with a VPN solution, which just adds to the complexity of the provisioning process. Features like Autopilot into co-management are also only supported with Entra ID joined, and not supported by Hybrid Autopilot.

Here are three very good reasons why you should not use Hybrid Autopilot:

- When you are doing device provisioning with Windows Autopilot, it uses only cloud services, but if you are using Hybrid Autopilot, you are leveraging cloud services that depend on an on-premises component. That can make it more complex with more moving parts.
- If you keep 100% of what you have today on-premises and add cloud components for provisioning, it is hard to realize any cost savings.
- Hybrid devices only prolong the journey to the cloud. There is no migration path from Microsoft from a hybrid device identity to a pure cloud device identity; therefore, a device reset or device reimaging is required to reach a cloud-native state at a later point.
- Microsoft recommends Entra ID join all new devices through Windows Autopilot.

What about existing infrastructure?

We talked about the broader unified endpoint management concept of Microsoft Intune in the first two chapters, explaining that you can manage and maintain all your devices from one single unified dashboard console.

We do recognize that not all customers are moving directly to Microsoft Intune in Entra ID with cloud-native devices. Therefore, co-managing existing on-premises Windows devices and Hybrid Entra ID-joined devices is also supported within Microsoft Intune. This creates the same unified endpoint management experience for your hybrid configuration.

Co-management and tenant attach

Co-management is not a new feature; it has been around for a while. Co-management makes it possible to move workloads from Configuration Manager (formerly **System Center Configuration Manager** (**SCCM**)) to Microsoft Intune. It tells the Windows clients that are managed by Configuration Manager who the management authority is (for different workloads) and also allows you to see and manage them from the Microsoft Intune console. To make it simple, a co-managed device is managed by both Configuration Manager and Microsoft Intune at the same time.

For example, with co-management, your existing Windows enterprise endpoints managed via Configuration Manager mainly listen to Configuration Manager for app deployment and security policies, while they look to Intune for compliance policies and device configuration policies. This helps businesses combine the benefits of both Configuration Manager and Microsoft Intune without making an impactful switch directly to Microsoft Intune.

Tenant attach is a bit different and limited in terms of management capabilities as tenant attach only makes it possible to add your Configuration Manager environment to Microsoft Intune, meaning you can leverage some of the Configuration Manager capabilities available in Microsoft Intune. Tenant attach allows you to perform actions on your Configuration Manager-managed clients using the **Microsoft Endpoint Manager** (**MEM**) portal, such as installing apps, running scripts, and so on.



IMPORTANT NOTE

To use co-management, you have to be using Configuration Manager version 2002 (at least).

In order to enable co-management within Configuration Manager, you must go through the **Co-management Configuration Wizard** screen to enable device upload.

Make sure to click **Sign in** and log on with a global administrator account.

The supported client OS versions for co-management are the following:

- Windows 11
- Windows 10

Make sure to select both of these options:

- **Upload to Microsoft Endpoint Manager admin center**
- **Enable automatic client enrollment for co-management**

The **Upload to Microsoft Endpoint Manager admin center** option enables tenant attach:

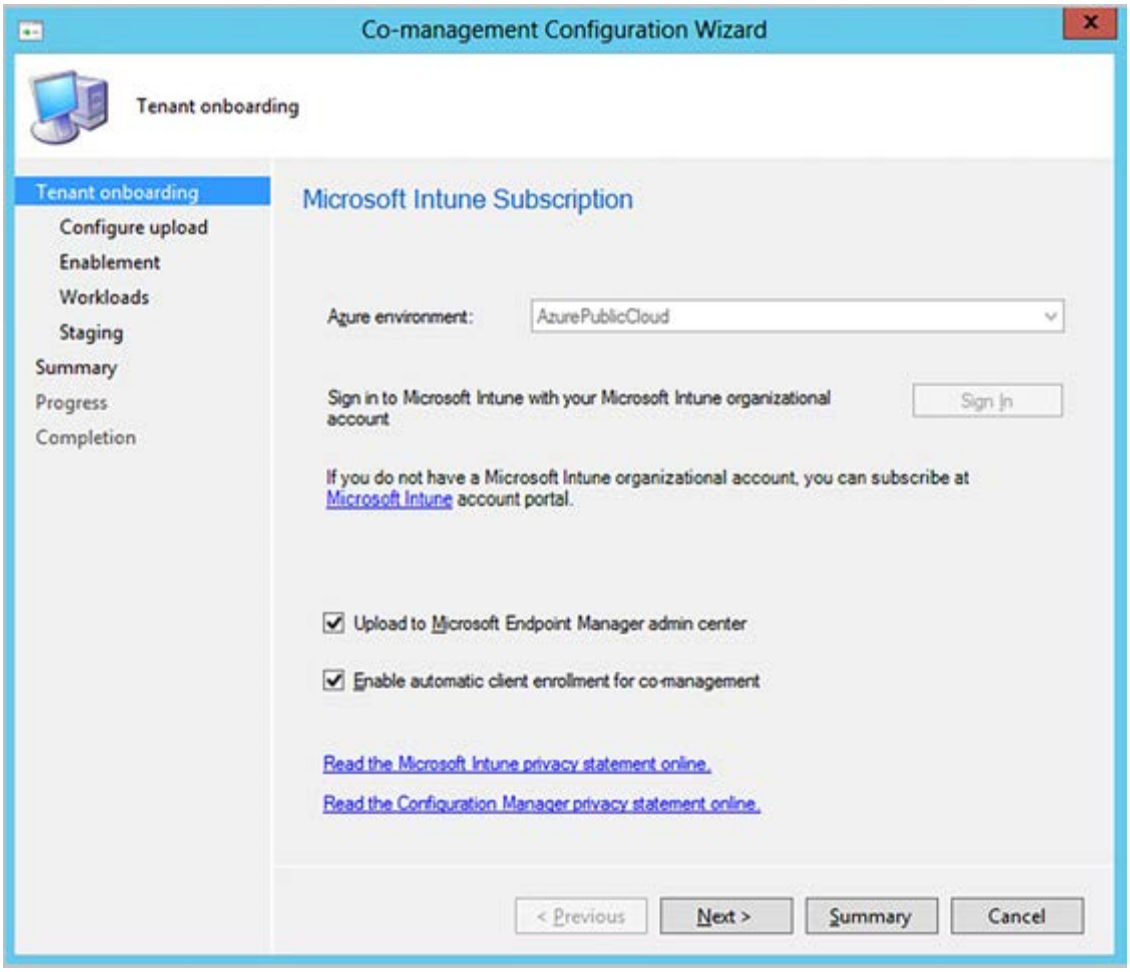


Figure 6.14: Co-management Configuration Wizard

In the following screenshot, make sure to enable the first setting if you want to add all your devices automatically to Microsoft Intune as co-managed devices. Alternatively, you can create collections to only add certain devices to the Microsoft Intune **Devices** menu instead; this is the second option in the following screenshot:

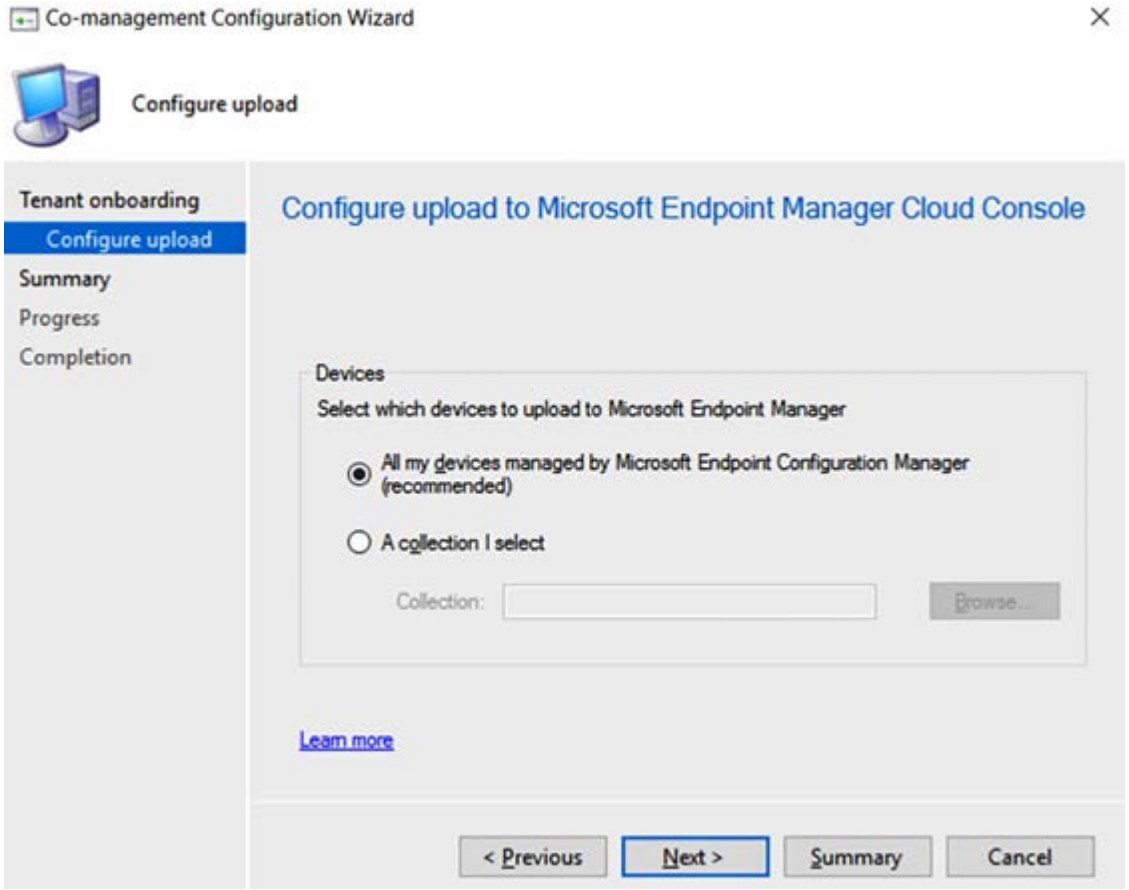


Figure 6.15: Co-management Configuration Wizard

After the setup, click **Next**, and the following completion confirmation should pop up on the screen to confirm that everything went as expected:

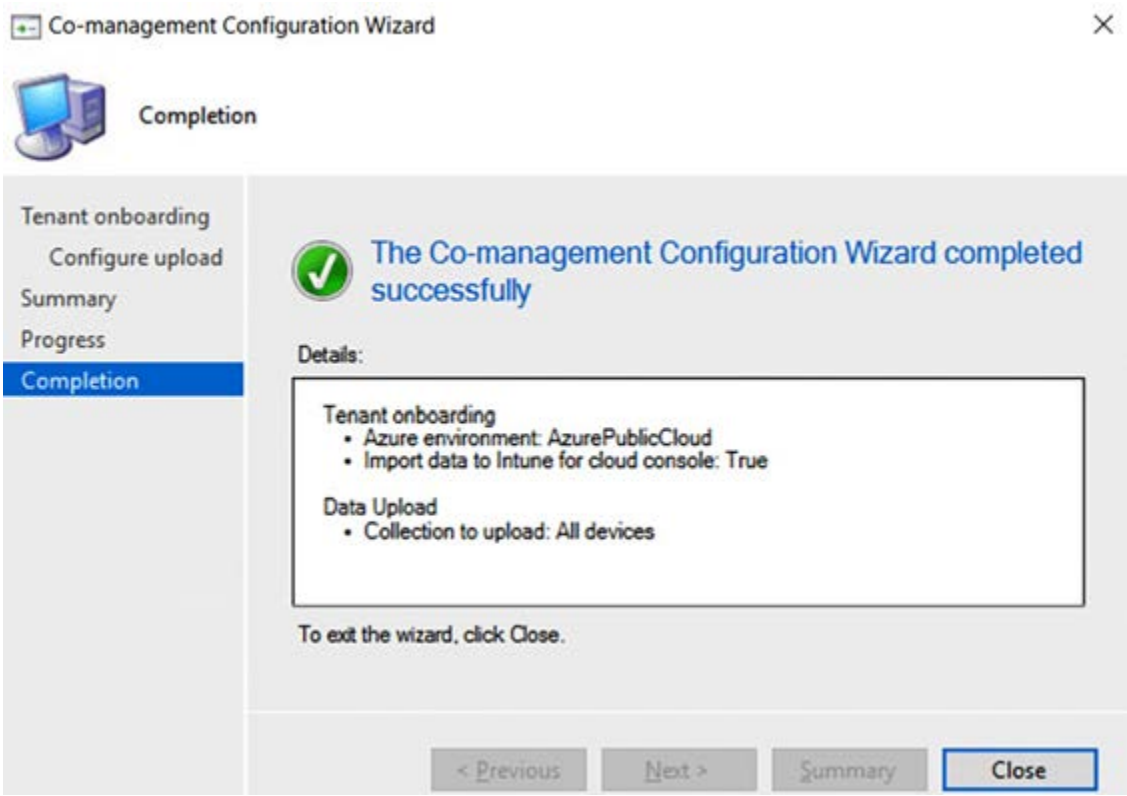


Figure 6.16: Co-management Configuration Wizard

The devices have now been added.

Also, make sure to select the **Enable Endpoint Analytics for devices uploaded to Microsoft Intune** option when you want to actively monitor your devices in Endpoint Analytics next to your Microsoft Intune-managed devices.

In the following screenshot, you can see how to upload device information from your Configuration Manager environment into Endpoint Analytics. You will learn more about Endpoint Analytics in *Chapter 14*, *Monitoring and Endpoint Analytics*:

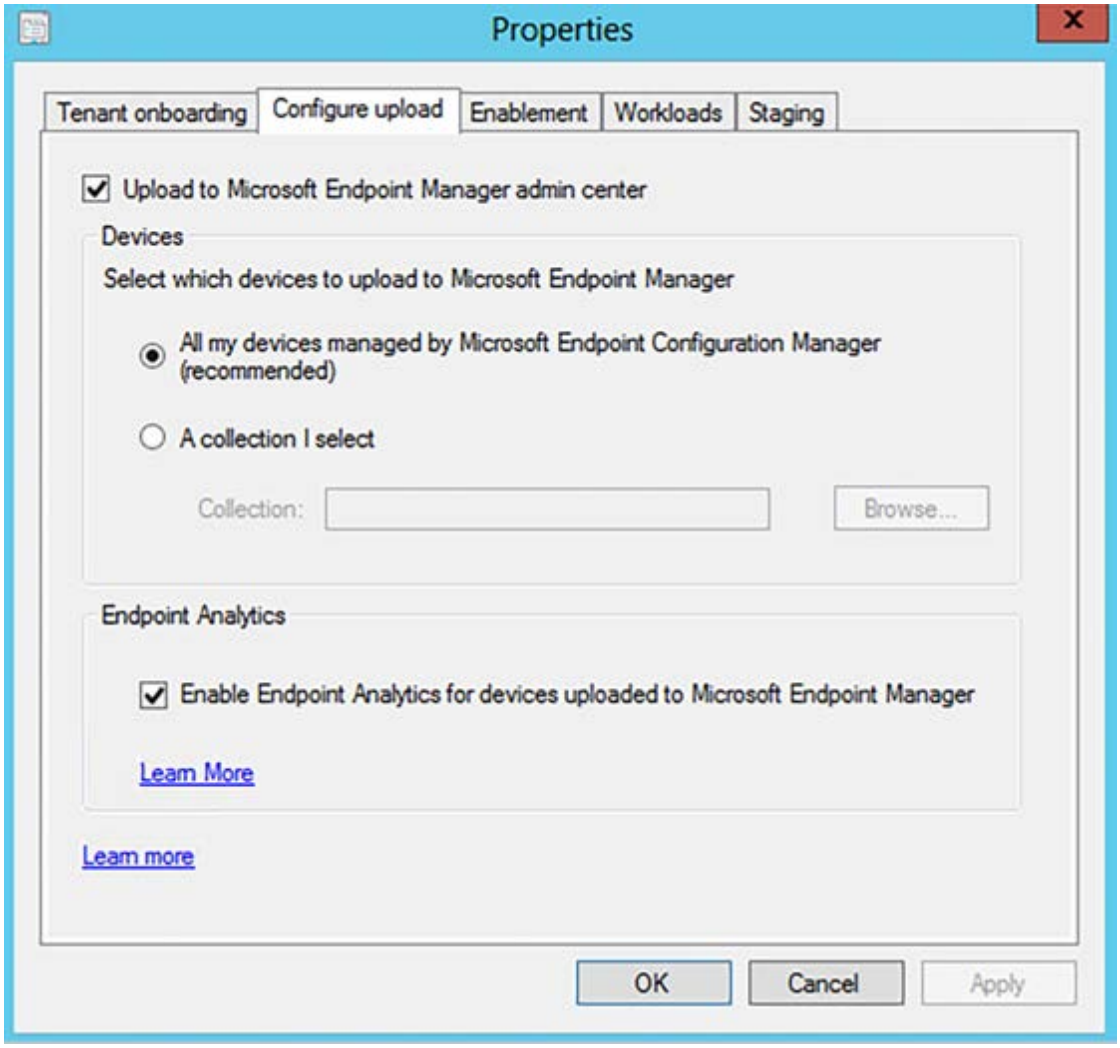


Figure 6.17: Endpoint Analytics upload setting

We'll talk about the benefits of Endpoint Analytics later on in the book in more depth where you will learn more about the added value in the context of monitoring.

After the wizard, in the Configuration Manager console, you'll see the connection to your Microsoft Intune tenant under **Cloud Services | Co-management**, as shown in the following screenshot:

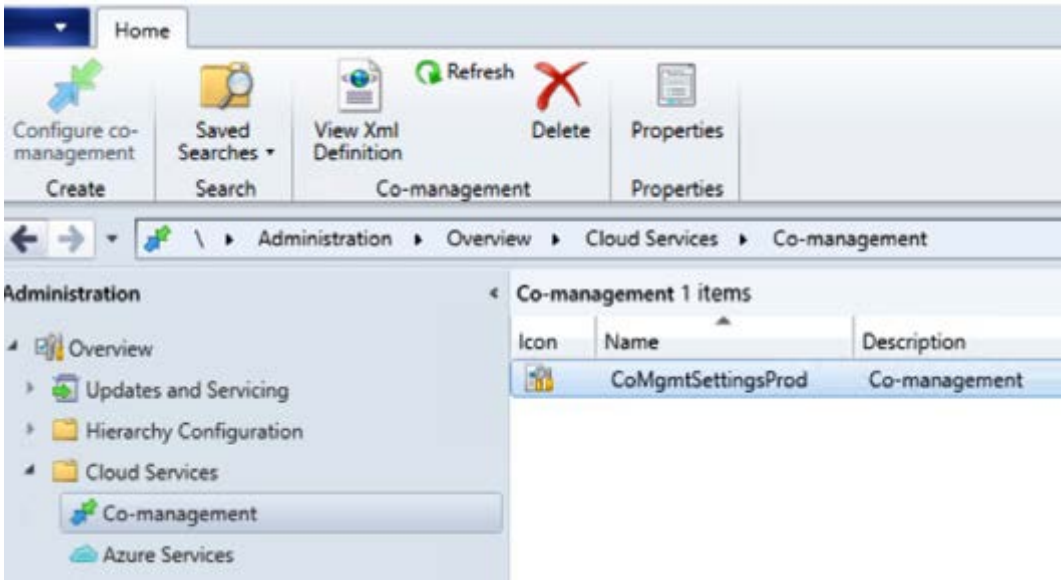


Figure 6.18: Co-management overview in Configuration Manager

If you do everything correctly, your devices will also show up in the Microsoft Intune admin center console, under **All devices:**

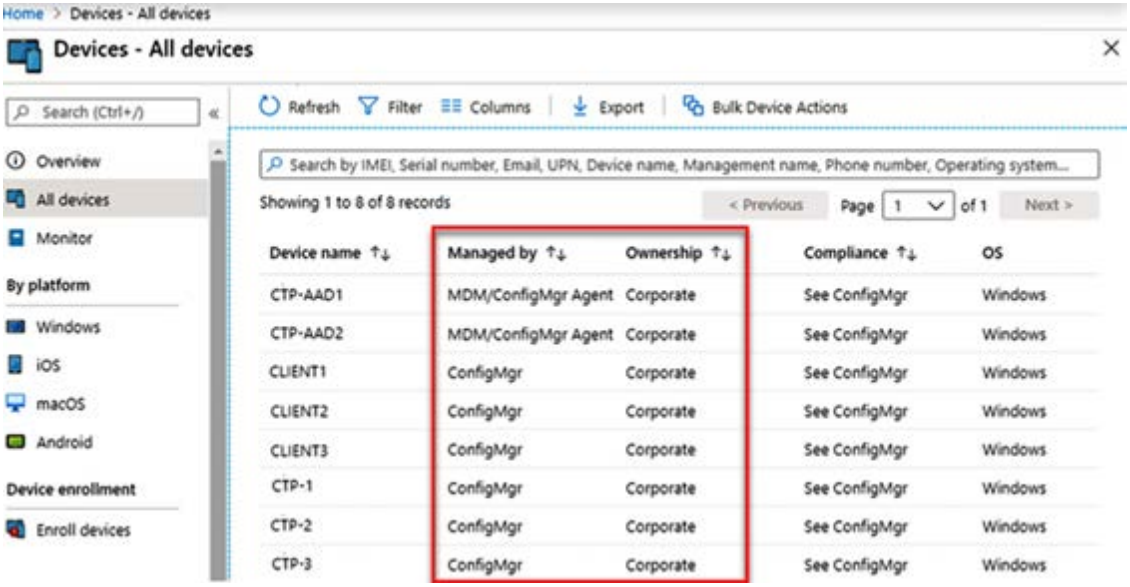


Figure 6.19: Device status in Microsoft Intune

If your devices do not show up in Microsoft Intune, start by troubleshooting your device state in Entra, your enrollment restrictions in Intune, your MDM authority in Intune, and so on.

Co-management settings

The co-management settings in Autopilot are a feature that allows you to configure brand-new devices using Windows Autopilot. The benefit of using the features is that when device provisioning is done, your devices are already co-managed and the workload is set to where you configured it. This feature is useful for organizations that want to combine the benefits of Intune for most workload management. When moving the client applications workload, apps from both Configuration Manager and Microsoft Intune will show up in Company Portal.

Some of the benefits of using co-management settings in Autopilot are:

- You can reduce the time, costs, and complexity of deploying, managing, and retiring devices by using the OEM-optimized version of Windows that's preinstalled on the device.
- You can automatically enable co-management by Intune during the Autopilot ESP phase of the first run experience. You don't need to create and assign an Intune Win32 app with the Configuration Manager binaries to install the Configuration Manager client.

To configure the co-management settings into Autopilot, do the following:

1. In the Microsoft Intune admin center, go to **Home** | **Devices** | **Windows enrollment** | **Co-management Authority** and click **Create**.
2. Configure and assign only one co-management policy.

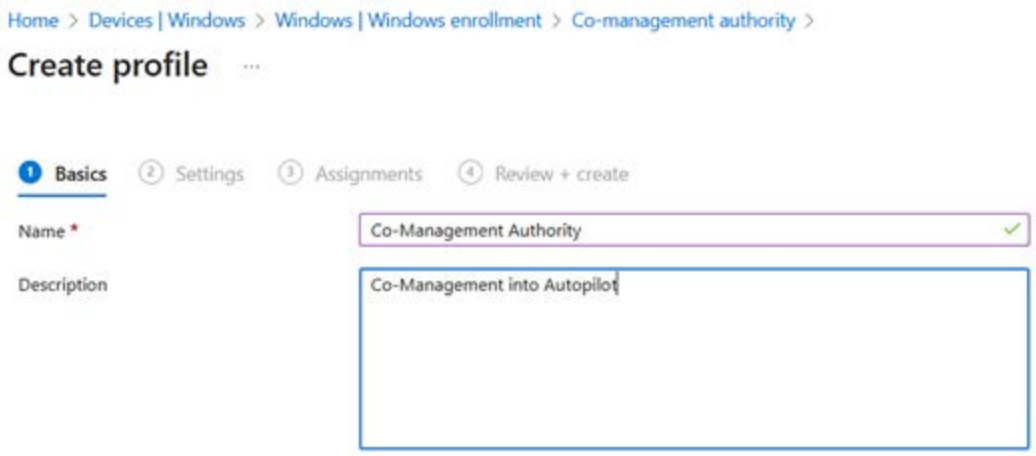


Figure 6.20: Co-Management Authority

3. Next, configure the co-management settings, as shown:

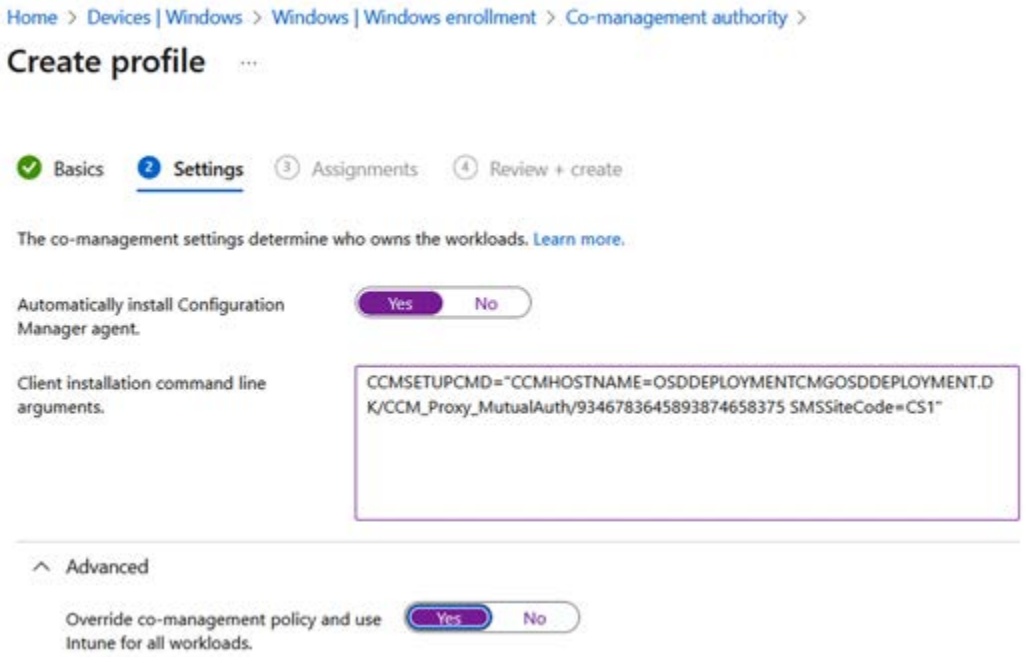


Figure 6.21: Co-management authority settings

4. The **Override co-management policy and use Intune for all workloads** option should be configured to **Yes**, so that when a device is done with the provisioning phase, all workloads will be in Microsoft Intune. One great example is compliance policies that will only apply in Intune and have the compliance state in Entra set to validate the device state with Conditional Access. Let's have a closer examination of the differences in toggling this **Yes/No** setting:

    - **Yes:** Intune is the authority and all workloads will be managed by Intune. That means that when a brand-new Autopilot instance is provisioned, Intune compliance policies will apply and determine whether the device is compliant or not. It will also affect other workloads like settings management, Windows Update, etc.
    - **No:** Configuration Manager will be the management authority and all workloads will be managed by Configuration Manager. This means that Configuration Manager will also manage the compliance policy, so if you are leveraging Conditional Access, your brand-new device will not be marked as compliant.

This concludes the section on the co-management settings for modern provisioning. In the next section, we will see an overview of Windows Update for Business.

Windows Update for Business

When you have devices that use Windows Update for Business to manage and control the update workflow, there are several policies that are of interest. We will cover them in this section. Update rings and features update policies are the basic policies that you, as the IT admin, should start configuring. To maximize the update velocity while remaining mindful of the impact on user productivity, Microsoft suggests a specific set of policies with recommended values. In this section, we will walk through these policies and how to configure them. Some of the benefits of using Windows Update for Business are:

- You can control the types of Windows updates that are offered to devices in your organization, such as feature updates, quality updates, cumulative updates, and optional updates.
- You can control when updates are applied to the devices, such as immediately after they are released, after a specified period of time, or after a specified date.
- You can deploy updates to devices in your organization in waves, testing them on a subset of devices before rolling them out to the rest of the organization.
- You can manage which updates are offered to devices based on their servicing channel, such as Windows Insider Preview or General Availability Channel.
- You can pause feature updates for up to 35 days after they are released to provide more time for testing and feedback.

Windows Update for Business policies, in this section, apply to Microsoft Intune or co-managed devices with the **Windows Update policies** workload set to **Microsoft Intune**.

Types of updates managed by Windows Update for Business

Windows Update for Business is designed to provide IT admins with the capability to manage policies for several types of updates to Windows devices:

- **Feature updates**: Previously referred to as **upgrades**, feature updates contain significant feature additions and changes along with security and quality revisions. Feature updates are released annually.
- **Quality updates**: Quality updates are traditional OS updates, typically released on the second Tuesday of each month, though they can be released at any time of the month. These include driver, security, and critical updates.
- **Driver updates**: These are updates for non-Microsoft drivers that are relevant to your devices. Driver updates are on by default, but you can use Windows Update for Business policies to turn them off if you prefer.
- **Microsoft product updates**: Windows Update for Business also treats non-Windows updates (such as updates for Microsoft Office, .NET, or Visual Studio) as quality updates. These non-Windows updates are known as **Microsoft updates** and you can set devices to receive such updates (or not) along with their Windows updates.

But first, how do Windows updates work? There are four phases to the Windows update process:

1. **Scan**: A device checks the Microsoft update server endpoint at random intervals to see whether any updates have been added since the last time updates were searched, and then evaluates whether the update is appropriate by checking the guidelines (for example, Intune policies) that have been set up by the administrator. This process is invisible to the user.
2. **Download**: Once the device determines that an update is available, it begins downloading the update. The download process is not visible to the user. The download happens in multiple sequential phases with feature updates.
3. **Install**: After the update is downloaded, depending on the device's configured Windows Update settings, the update is installed on the system.
4. **Commit and restart**: Once the update is installed, often the device must be restarted (not all Windows updates require an update to be applied and have an effect on Windows) in order to complete the installation and begin using the update. Before this phase, the device is still running the previous version of the software.

At each stage of the process, there are opportunities to increase the velocity via policies and settings, and our recommendations follow.

Enforcing compliance deadlines for updates

Deploying feature or quality updates for many organizations is only part of the equation for managing their device ecosystems. The next important part is the ability to enforce update compliance. Windows Update for Business provides controls to manage deadlines for when devices should migrate to newer versions.

How to handle conflicting or legacy policies

We sometimes find that administrators set devices to get both Group Policy settings and MDM settings from an MDM server such as Microsoft Intune. Depending on how they are ultimately set up, policy conflicts are handled differently:

- **Windows Updates**: Group Policy settings take precedence over MDM.
- **Microsoft Intune**: If you set different values for the same policy on two different groups, you will receive an alert and neither policy will be set until the conflict is resolved.

It is crucial that you disable conflicting policies for devices in your organization to update as expected. For example, if a device is not reacting to your MDM policy changes, check to see whether a similar policy is set via Group Policy with a differing value. When you enable co-management and move the Windows Update workload from Configuration Manager to Intune, keep in mind that it does not automatically clean up existing settings on the device.

If you find that the velocity is not as high as you expect or some devices are slower than others, it may be time to clear all policies and settings and specify only the recommended update policies outlined in this chapter.

How to set up and configure Windows Update for Business

Before you begin configuring Windows Update for Business policies in Microsoft Intune, you should start with configuring Windows diagnostics data settings to ensure that all policies and reports work as you expect. To configure Windows diagnostics data, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Tenant administration** | **Connectors and tokens** | **Windows data**.
2. Toggle the **Enable features that require Windows diagnostic data in processor configuration** setting to **On**. Additionally, under **Windows license verification**, where it says **I confirm that my tenant owns one of these licenses**, move the toggle to **On** if you have the correct licenses for those features to be enabled in your Intune tenant.

Windows diagnostic data processor configuration enables you to be the controller, as defined by the European Union **General Data Protection Regulation** (**GDPR**), for the Windows diagnostic data collected from your Windows devices that meet the configuration requirements.

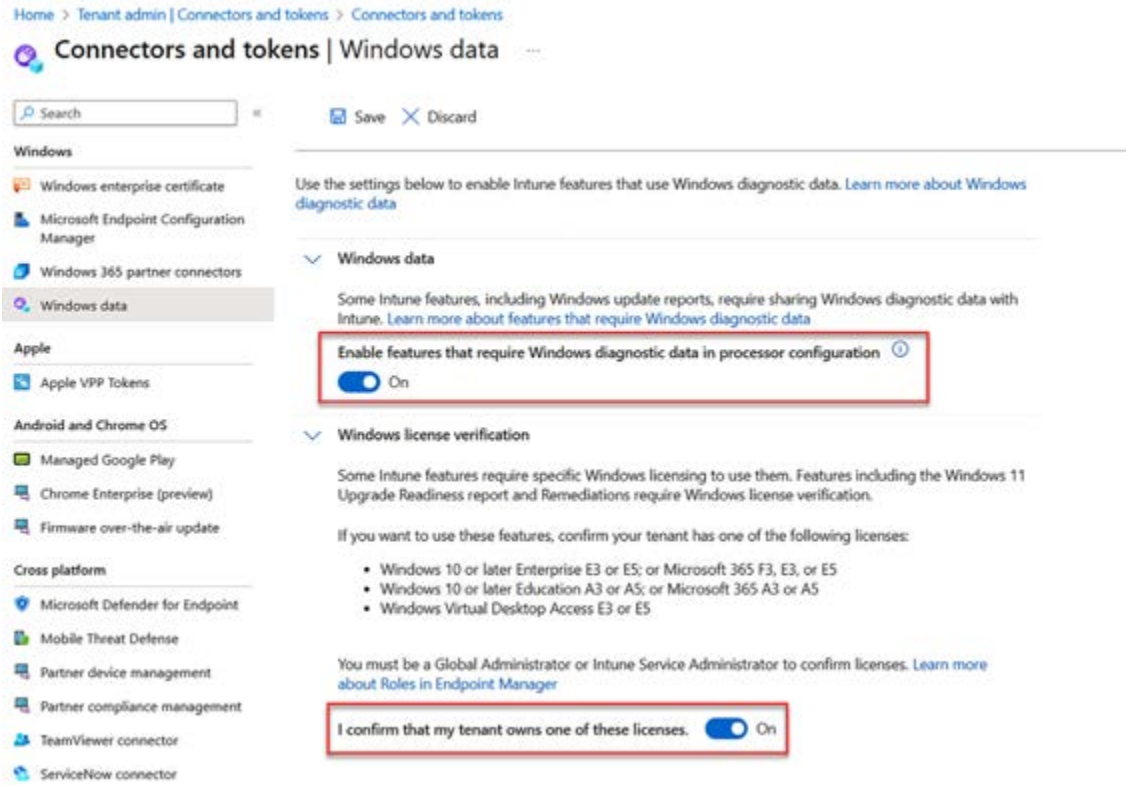


Figure 6.22: Windows data

Now that we have configured Windows diagnostics data, we can move forward with configuring Windows Update for Business policies in Microsoft Intune.

The steps to set up and configure Windows Update for Business in Microsoft Intune are as follows:

1. In the Microsoft Intune admin center, go to **Devices** | **Windows** | **Update rings for Windows 10 and later** | **Create profile:**

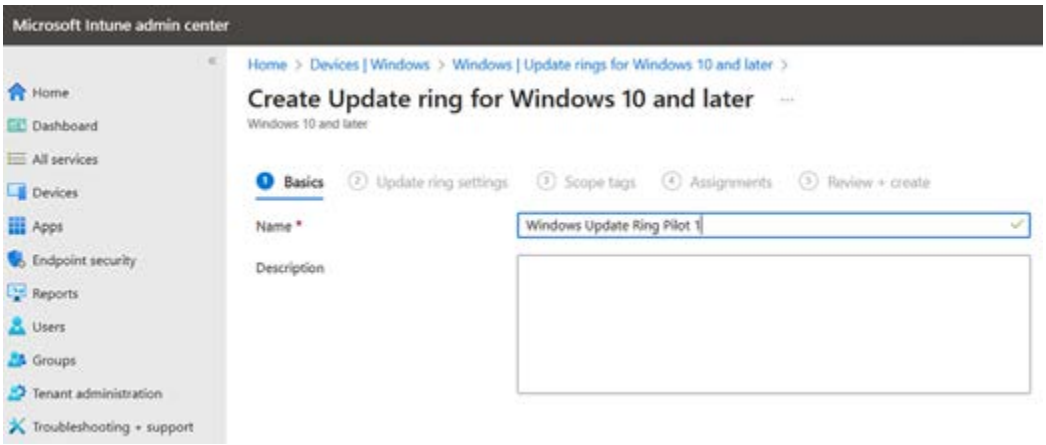


Figure 6.23: Create Update ring for Windows 10 and later

2. In the **Update settings** section, **Upgrade Windows 10 devices to Latest Windows 11 release** is needed for Windows 10 Pro to allow upgrade to Windows 11. Here, enable the toggle to **Yes**. For Windows 10 Enterprise, we recommend leveraging feature updates for Windows 10 and later that are built on top of the Windows Update for Business deployment service.

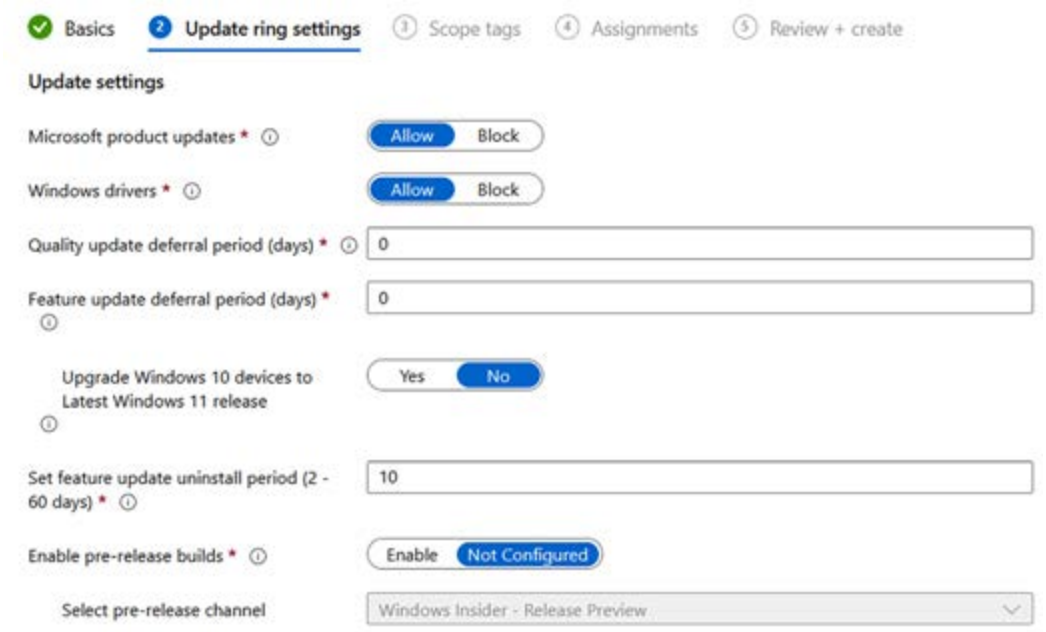


Figure 6.24: Create Update ring for Windows 10 and later

3. For **Enable pre-release builds**, Microsoft Intune automatically configures the Windows Update settings so that Windows Insider builds will work. We'll see more about Windows Insider for Business in a later section.

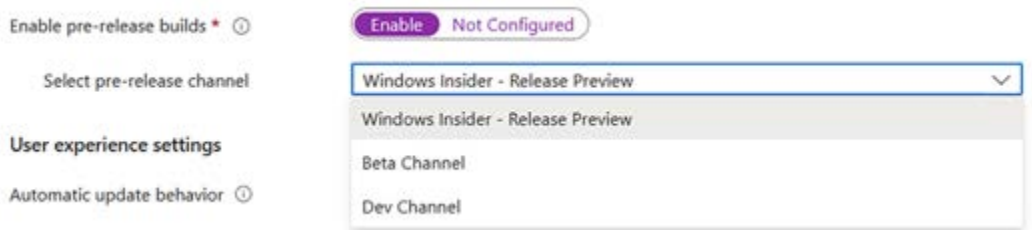


Figure 6.25: Enable pre-release builds

Here's a breakdown of the different configuration settings for pre-release builds:

- **Windows Insider - Release Preview**
- **Beta Channel**
- **Dev Channel**

An IT administrator can defer the installation of both feature and quality updates from deploying to devices within a bounded range of time from when those updates are first made available on the Windows Update service.

This deferral can be used to allow time to validate deployments as and when they are pushed to devices.

Deferrals work by allowing you to specify the number of days after an update is released before it is offered to a device. In this way, you can create a ring deployment with different deferral days for the following:

- Pilot group
- Production ring 1
- Production ring 2
- Broad deployment

The update release rings are visualized in the following diagram to help you understand the order better. Start in the **Plan & Develop** section, where you create a plan for how you want to update your Windows estate and the number of days you want set your quality update deferral period to, then create the necessary Windows Update rings that match your plan:



Figure 6.26: Windows Update release rings

When moving to servicing-based Windows updates, you need controlled ways of rolling out updates to representative groups of devices. Deployment rings in Windows are like the deployment groups most organizations have used in the past with other deployment tools; deployment rings are simply a method to separate groups of machines into a controlled deployment timeline.

You can create as many deployment rings as you need and assign them to different device groups. Keep in mind that you don't want conflicting rings assigned to the same devices. You assign policies for update rings for Windows 10 and later and feature updates for Windows 10 and later to groups of devices.

You can set a feature update deferral period of 365 days; the device will not install a feature update that has been released for less than 365 days. This is a great option if you want to be 100% in control of the feature updates that are being installed on your corporate devices or if you want to skip feature updates and only apply them once a year to your corporate devices.

In the following table, you can find the settings you can configure with the deferral period time per category:

Category	Maximum deferral period	Suggested configurations
Feature updates	365 days	7
Quality updates	30 days	7
Non-deferrable	None	N/A

Non-deferrable Windows updates refer to specific types of updates that cannot be postponed or deferred by the user. These updates are critical for maintaining the security and stability of your Windows operating system. Here are the key points about non-deferrable updates:

1. **Antimalware and antispyware definition updates**: These updates, which protect your system from malware and spyware, fall into the non-deferrable category. They are essential for keeping your device secure and cannot be delayed.
2. **Optional updates**: While most updates can be deferred, starting from November 2023, Windows 10 devices will have the option to receive optional non-security updates automatically. These updates include gradual feature rollouts and other non-critical enhancements. Organizations can configure policies to control how these optional updates are made available to users:
    a. Automatically receive optional updates (including CFRs): This option ensures devices get the latest optional non-security updates, including gradual feature rollouts.
    b. Automatically receive optional updates: Devices receive only the latest optional non-security updates without gradual feature rollouts.
    c. Users can select what optional updates to receive: Users can set their own preferences for optional non-security updates.
3. **Quality updates and drivers**: While not explicitly labeled as "non-deferrable," quality updates (which include security patches) and drivers are typically installed day-one of release. These updates are crucial for maintaining system reliability and performance.

    For **Microsoft product updates**, the default selection is **Allow**. The two available options are as follows:

    - **Allow**: Select **Allow** to scan for app updates from Microsoft Update.
    - **Block**: Select **Block** to prevent scanning for app updates.



TIP

The recommended value is **Allow** so that you keep all Microsoft products that are installed on the device updates, such as C++, .NET, and so on.

For **Windows drivers**, the default selection is **Allow**. The two options available are as follows:

- **Allow**: Select **Allow** to include Windows Update drivers during updates.
- **Block**: Select **Block** to prevent scanning for drivers.



TIP

The recommended value is **Allow** so that you keep all your drivers updated directly from Windows Update, both for security-related fixes in drivers and firmware as well as stability – be aware that this is an **on/off** switch for enabling or disabling all-or-nothing driver updates from Windows Update.

Ensure that **Windows drivers** is set to **Allow** if you want to leverage driver and firmware updates in a controlled way.

4. **Set feature update uninstall period (days) (2 - 60 days)** allows you to set the number of days you can remotely uninstall a feature update from a device.
5. From within your update ring policy in Microsoft Intune, you can choose to uninstall a Windows feature or quality update on devices.

   See the following screenshot for how you can uninstall either feature or quality updates from the Microsoft Intune admin center:

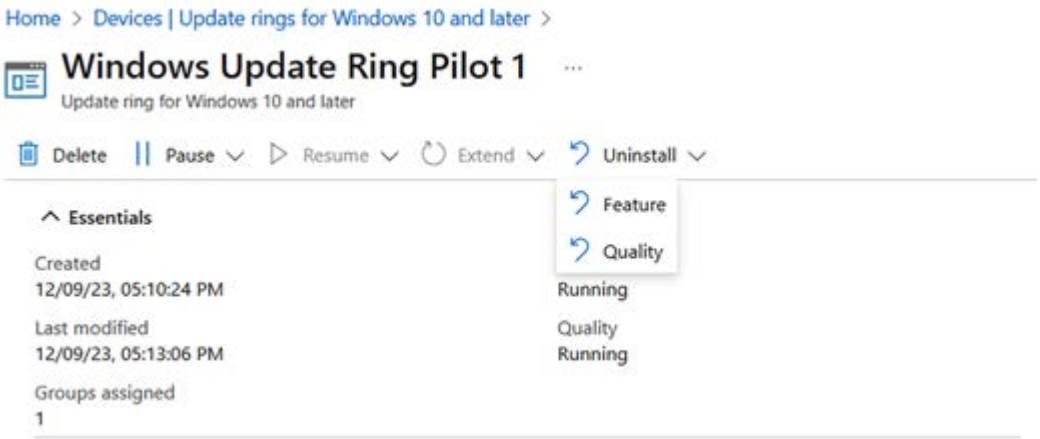


Figure 6.28: Update ring policy

6. In the **User experience settings** section, you can create the user experience behavior around applying updates.

   The following screenshots shows the default settings for a Windows Update for Business policy in Intune, which also specifies Windows' active hours from 8 A.M. to 5 P.M. unless you change it in the policy:

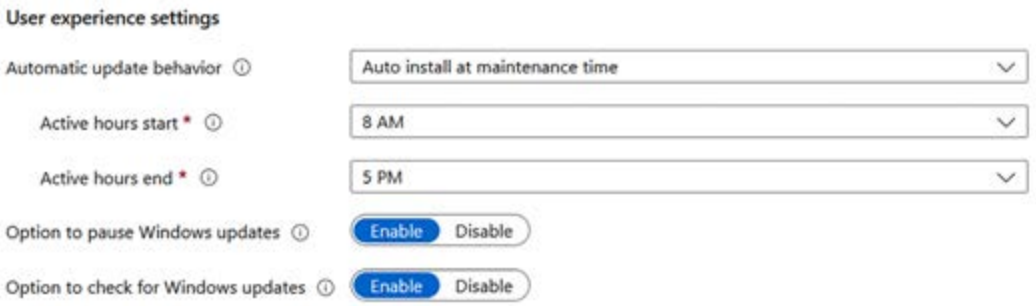


Figure 6.29: Update ring policy active hours



Figure 6.30: Update ring policy – Reset to default

By using **Reset to default** instead, which is the Microsoft-recommended setting, your end users can set active hours themselves and the system will leverage intelligent active hours if the end user does not configure active hours directly. This is more important than ever when employees are working different hours than before working from home became the new normal:

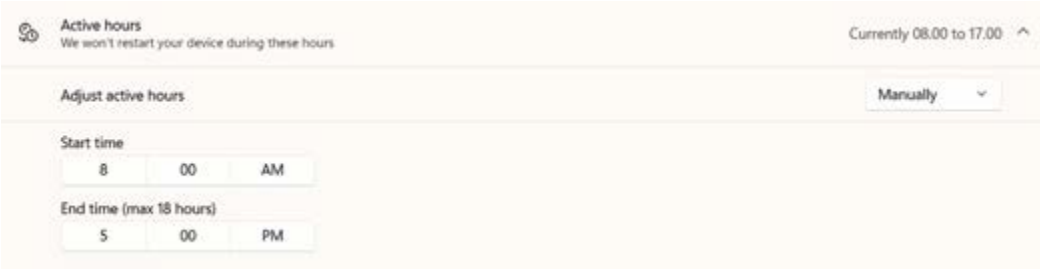


Figure 6.31: Active hours client side

Restart checks can be set to skip all checks before restarting. This includes the battery level being at 40%, the user presence, the display needed, presentation mode, fullscreen mode, phone call state, game mode, and so on.

Option to pause Windows updates gives the end user the option to pause an update from Windows Update for up to 7 days.

If you discover a problem while deploying a feature or quality update, it can be paused by the IT administrator for 35 days from a specified start date to prevent other devices from installing it until the issue is mitigated. If you pause a feature update, quality updates are still offered to devices to ensure they stay secure. The pause period for both feature and quality updates is calculated from the date when you pause the policy.

From within your update ring policy in Microsoft Intune, you can choose to pause Windows feature or quality updates on devices:

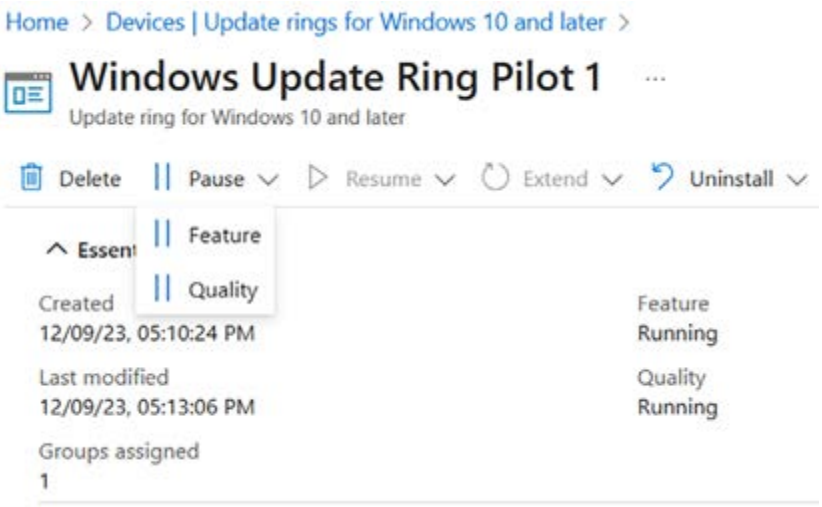


Figure 6.32: Pause Windows updates

If you have configured the Option to pause Windows updates setting in the update ring, the end user can pause updates using the **Settings** app on Windows. See the following screenshot with the option to pause updates.

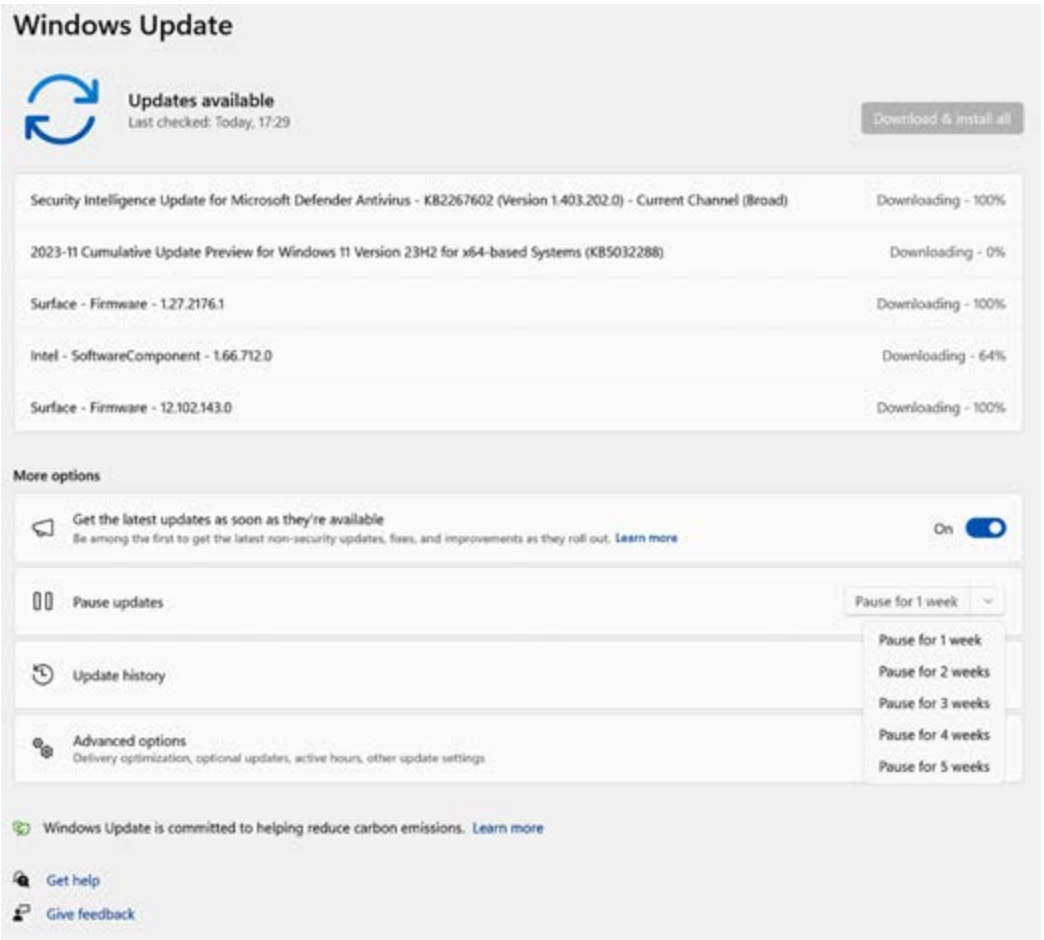


Figure 6.33: Pause Windows updates

The end user can pause Windows updates from the Settings app for up to 5 weeks.

Option to check for Windows updates is a setting in Windows Update that, when enabled, lets device users check the update service for updates.

For **Require user approval to dismiss restart notification**, specify the method by which the auto-restart required notification is dismissed. For the best end user experience, set this to **Yes**, but when your end users are in control, it can slow down the update rollout on your devices. It is recommended to leave it as the default: **No**. You can find the settings in the following screenshot:

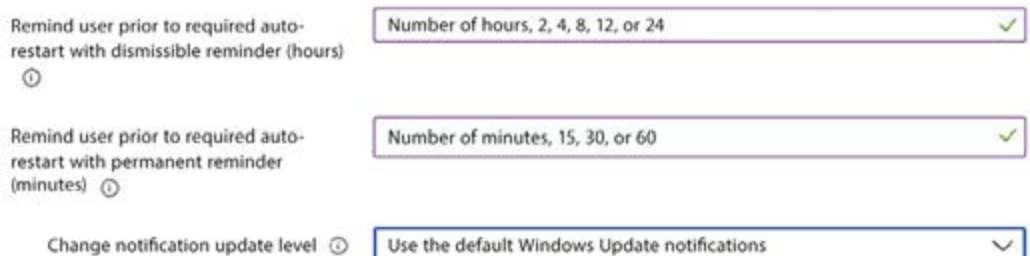


Figure 6.34: Update ring policy

For **Remind user prior to required auto-restart with dismissible reminder (hours)**, specify the period for auto-restart warning reminder notifications. Allowed values are **2**, **4**, **8**, **12**, or **24**. The default value is 4 hours. The recommendation is to leave it blank.

For **Remind user prior to required auto-restart with permanent reminder (minutes)**, specify the period for auto-restart imminent warning notifications. Allowed values are **15**, **30**, or **60**. The default value is **15**. The recommendation is to leave it blank.

Change notification update level specifies what Windows Update notifications users see. The recommendation is to set it to **Use the default Windows Update notifications**, so that the end user gets as many notifications as possible and has the option to take action on this accordingly.

If you have a Kiosk device, an ATM, or another device with no user on it, it is recommended to set it to **Turn off all notifications, including restart warnings**, as there are no end users to respond to the notifications on those devices. You can find the settings in the following screenshot:



Figure 6.35: Update ring policy notification level

7. **Use deadline settings** allows you to leverage deadline settings. The recommended setting is **Allow**. Leveraging the **Allow** setting gives you, as an IT administrator, the option to set deadlines for both feature and quality updates.

   For **Deadline for feature updates**, the number of days allowed is 2 to 30. It is recommended to set it to **7**, so a Windows feature update will have a deadline of 7 days before it is forced to do the installation and reboot.

   For **Deadline for quality updates**, the number of days allowed is 2 to 30. It is recommended to set it to **5**, so a Windows quality update will have a deadline of 5 days before it is forced to do the installation and reboot. This does not prevent the end user from installing the quality updates before the deadline has been reached.

   For **Grace period**, the number of days allowed is 0 to 7. It is recommended to set it to **2** days, so if an end user comes back from vacation, they will have 2 days to get the updates installed and restart their device.

For **Auto reboot before deadline**, the recommended setting is **Yes.** This specifies whether the device should auto-reboot before the deadline. **Yes** will ensure that the reboot happens with as little end user interaction as possible. **No** will ensure that the end user is always present on the devices for a reboot.

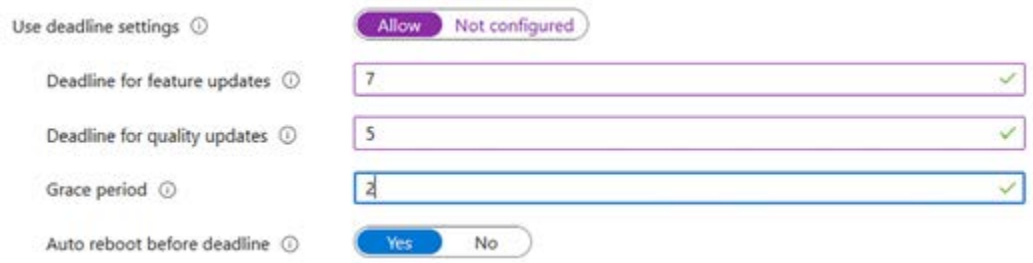


Figure 6.36: Update ring policy – Use deadline settings

When you specify different deadlines for automatic Windows updates and OS restart, the end user notifications will look like this:

- The user receives a toast notification, a few days after which the user receives this dialog:



Figure 6.37: Toast notification

- The user receives this notification 15 minutes before the restart if the user scheduled a restart or if an auto-restart is scheduled:

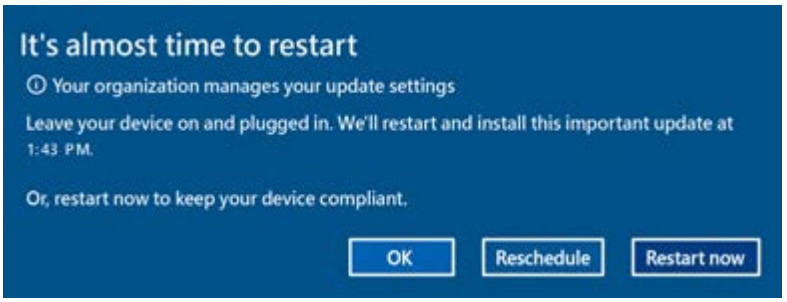


Figure 6.38: Restart notification

If the restart is still pending after the deadline passes, the following notifications are shown:

- 12 hours before the deadline passes, the user receives this notification:

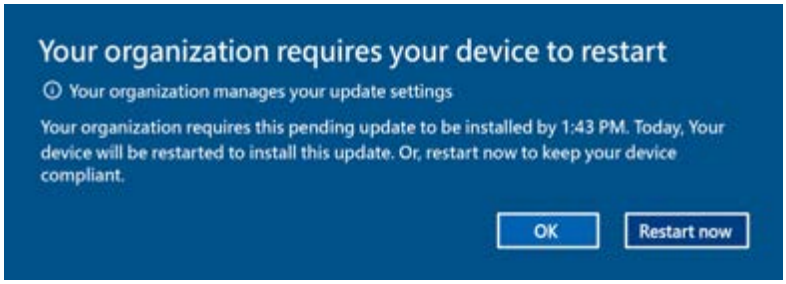


Figure 6.39: Notification before deadline passes

- The user is forced to restart to keep their devices in compliance once the deadline has passed and receives this notification:

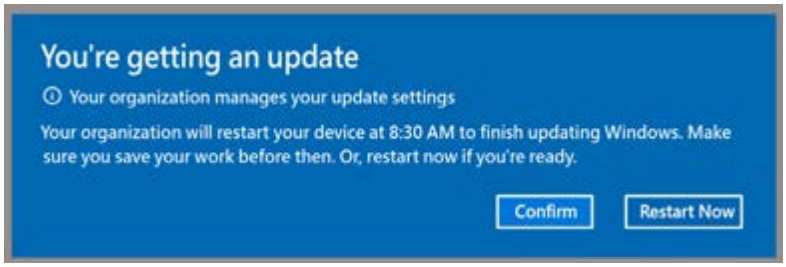


Figure 6.40: Notification after deadline passes

For the best experience with Windows Update, follow these guidelines:

- Use devices for at least 6 hours per month, including at least 2 hours of continuous use.
- Keep devices regularly charged. Plugging in devices overnight enables them to automatically update outside of active hours.
- Make sure that devices have at least 10 GB of free space (enable the Storage Sense policy).
- Give devices unobstructed access to the Windows Update service.

The next section will explain everything you need to know about preventing updates to devices that include known issues. Let's take a look.

Safeguard holds

Safeguard holds prevent a Windows device with a known issue from being offered a new feature update. Microsoft renews the offer once a fix is found and verified. Microsoft uses safeguard holds to ensure customers have a successful experience as their device moves to a new version of Windows. An example is a hardware driver that is not ready for the next Windows version, so the safeguard hold prevents that device from being upgraded until there is a working driver released.

The time for which safeguard holds apply to a specific Windows device or hardware model varies depending on the time required to investigate and fix an issue. During this time, Microsoft works diligently to procure, develop, and validate a fix and then offer it to the affected devices. Microsoft monitors quality and compatibility data to confirm that a fix is complete before releasing the safeguard hold. Once Microsoft removes the safeguard hold, Windows Update will automatically resume offering the Windows feature update that was on the safeguard hold. A safeguard hold is not the same as an IT administrator-leveraged pause in a Windows Update for Business deployment ring.

The aim of safeguard holds is to protect the device and user from a failed or poor upgrade experience.

When using Windows Update for Business and a device has a safeguard hold, the end user will see the following message in the Windows Update part of the local settings app on a Windows 10 device:



Figure 6.41: Feature update

As there is a reason for safeguard holds, it is not recommended to manually attempt to upgrade Windows until the issue that is causing the safeguard hold is resolved.

Feature updates for Windows 10 and later

Feature updates for Windows 10 and later policies work in conjunction with your Update rings for Windows 10 and later policies from Microsoft Intune, to prevent a device from receiving a Windows feature version that is later than the specified Windows version in the feature updates policy. Feature updates for Windows 10 and later leverage the Windows Update for Business deployment service.

The Windows Update for Business deployment service is a cloud service that allows you to control the approval, scheduling, and safeguarding of updates delivered from Windows Update to your managed devices. It is designed to work with your existing Windows Update for Business policies and reports, and it provides a direct communication channel between a management tool and the Windows Update service. You can use the deployment service to approve and schedule specific updates for deployment, such as feature updates, quality updates, security updates, driver updates, and more. You can also use the deployment service to deploy driver updates that are tailored to your population based on diagnostic data.

To use the Windows Update for Business deployment service, you need to meet some prerequisites, such as having an Azure subscription with Microsoft Entra ID, having one of the supported licenses for Windows 10/11 Enterprise or Education editions, having diagnostic data enabled on your devices at the **Required** level or higher, and having the appropriate permissions. You can also use various tools to interact with the deployment service, such as PowerShell, Microsoft Graph apps, or Microsoft Intune. For example, you can use Graph Explorer to make requests to the Microsoft Graph APIs to approve or schedule feature updates.



NOTE:

If you use Microsoft Graph APIs to create and/or manage policies in the Windows Update deployment service, those policies will not be visible in Intune. But policies created in Intune can we viewed with the Graph API.

The Windows Update deployment service complements existing Windows Update for Business capabilities, such as client policy and reports. It gives you more flexibility and control over how you manage update deployments on your devices.

When using feature updates for Windows 10 and later policies, the feature update setting in the Windows update ring policy should be configured to **0**, which you can do with the following setting in Microsoft Intune:



Figure 6.42: Update ring policy setting

Feature updates for the update ring must be running. They must not be paused.

The device updates to the version of Windows specified in the policy. However, it remains at its current version if the device is already running a later version of Windows. By freezing the version, the device's feature set remains stable for the duration of the policy.

Windows feature updates require the following prerequisites:

- Be enrolled in Intune MDM and be Hybrid Entra-joined or Entra ID joined.
- Have **Telemetry** turned on, with a minimum setting of **Basic**.

To configure feature updates for Windows 10 and later, follow these steps:

1. In the Microsoft Intune admin center, go to **Devices | Windows | Feature updates for Windows 10 and later | Create profile:**

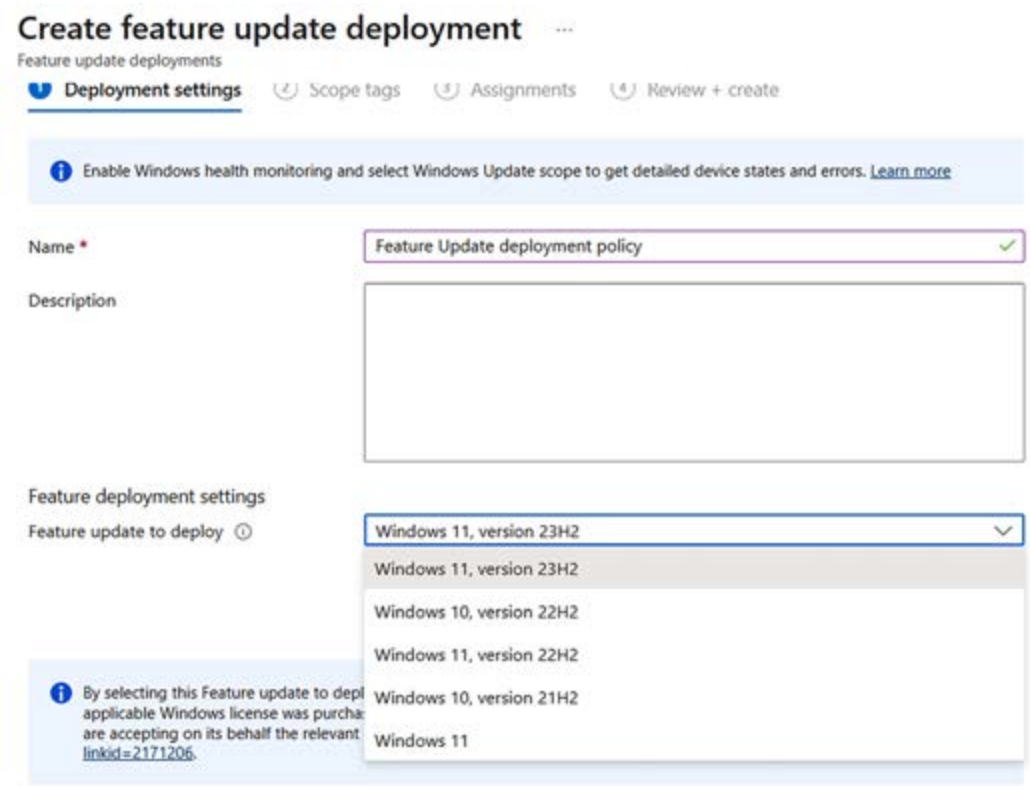


Figure 6.43: Create feature update deployment

You can select feature updates to be deployed as follows (the list will always show the currently supported OS versions):

- **Windows 11, version 23H2**
- **Windows 10, version 22H2**
- **Windows 11, version 22H2**
- **Windows 10, version 21H2**
- **Windows 11**

By setting this policy, the specified Windows feature is not downloaded and installed from Microsoft Intune, but rather, it tells the devices to send information on what feature update the devices should be on when Windows Update sync is performed at the next scheduled time after receiving the policy from Microsoft Intune.



Figure 6.44: Feature update deployment

2. If you have devices that aren't eligible to run Windows 11, you can check this setting to always install the latest Windows 10 feature update.
3. You have the option to decide between three different rollout options:

    a. **Make update available as soon as possible**

    Here, the feature update will be available as soon as possible to the devices that the policies are assigned to.



Figure 6.45: Make update available as soon as possible

    b. **Make update available on a specific date**

    To make the feature update available on a specific day, you can select the **Make update available on a specific and date** option, and then select a specific day when you want the Windows feature update to be available in Windows in the targeted devices.

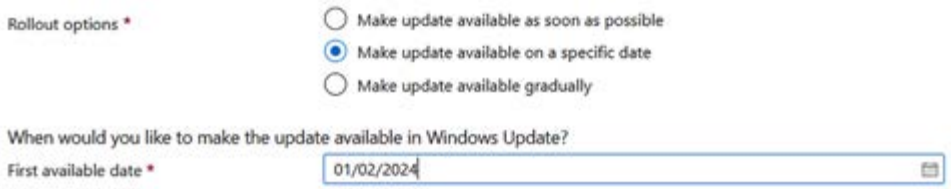


Figure 6.46: Make update available on a specific date

    c. **Make update available gradually**

    Selecting the **Make update available gradually** option means that the Windows feature update will be available to the first group on a specific day that you configure. You select the day when the final group will receive the update and the number of days between the groups.

Windows Update will then automatically create groups to match the configuration that you have provided, dividing your assigned devices between the groups.

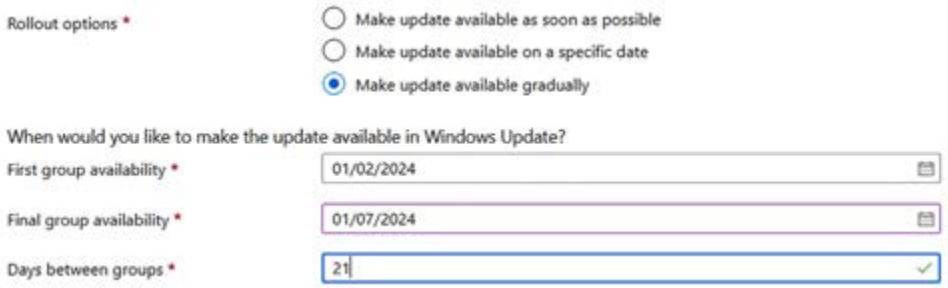


Figure 6.47: Make update available gradually

4. With gradual rollouts, you can also configure intelligent rollouts. This means the Windows Update for Business deployment service uses data collected from your devices to determine the most optimized device members in each group. This requires the **Allow WUfB Cloud Processing** policy to be configured on your devices. This can be done by creating a **settings catalog** policy.



Note: This setting is not in the **Update/Feature/Quality/Driver update** ring sections. You need to create a settings catalog policy yourself and assign it to your device group.

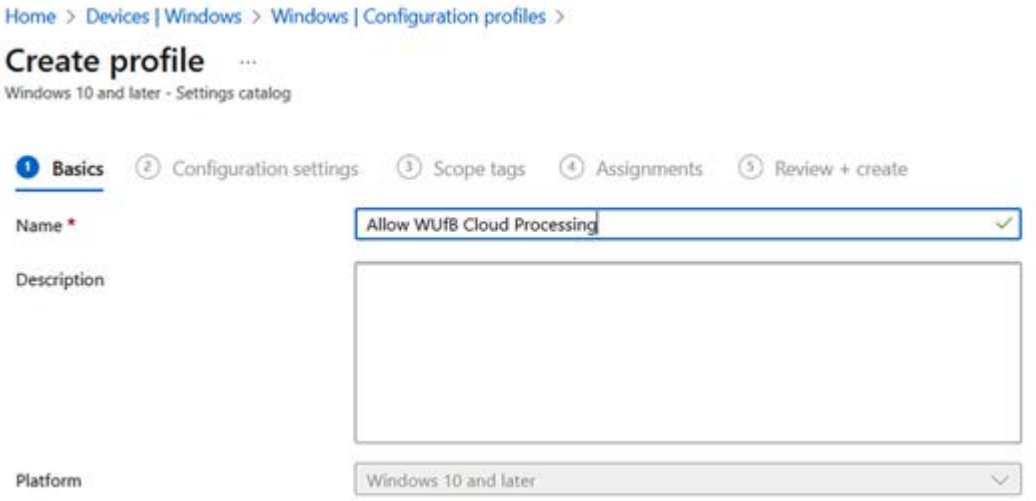


Figure 6.48: Allow WUfB Cloud Processing

5. Search for the **Allow WUfB Cloud Processing** setting and configure it to **Enabled**.

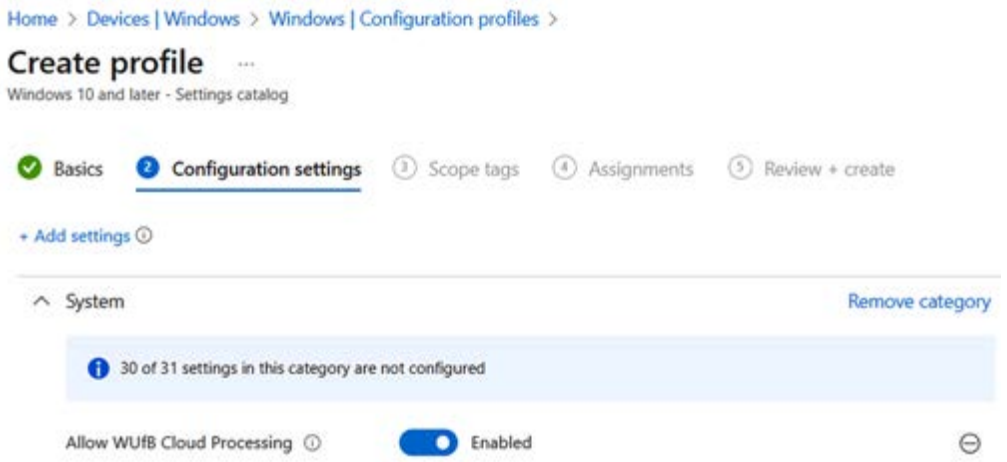


Figure 6.49: Allow WUfB Cloud Processing – Enabled

Allow WUfB Cloud Processing enables the processing of diagnostic data from this device by the Windows Update for Business cloud. The following list shows the supported values:

- **0 (default)** – Diagnostic data is not processed by the Windows Update for Business cloud.
- **8** – Diagnostic data is allowed to be processed by the Windows Update for Business cloud.

If you disable or do not configure this policy setting, diagnostic data from this device will not be processed by the Windows Update for Business cloud.

Opting out of safeguard holds

Opting out of Windows Update safeguard holds is available on Windows Update for Business devices running Windows 10 version 1809 and above with the October 2020 security update installed.

Safeguard holds prevent a device with a known compatibility issue from being offered a new OS version. The offering will proceed once a fix is issued and is verified on a held device.

The safeguard holds protection is provided by default to all devices trying to update to a new Windows 10 feature update version via Windows Update.

IT admins can, if necessary, opt devices out of safeguard protections using Group Policy settings or, via the **Disable safeguards for Feature Updates** MDM settings, create a settings catalog policy to opt out of the safeguard hold. Opting out of safeguards is not recommended on production devices.

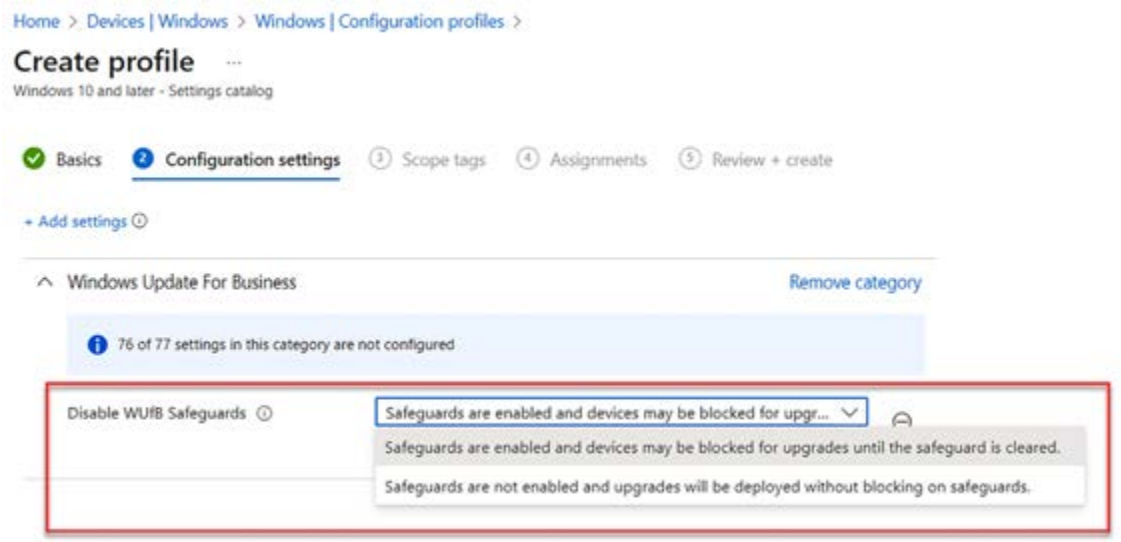


Figure 6.50: Disable WUfB Safeguards

The supported values for this option are as follows:

- (default) **Safeguards are enabled and devices may be blocked for upgrades until the safeguard is cleared.**
- **Safeguards are not enabled and upgrades will be deployed without blocking on safeguards.**

Opting out of the safeguards can put devices at risk of known performance issues. The recommendation is only opting out in an IT-controlled environment for validation purposes.

The **Disable safeguards policy** option will revert to **Not Configured** on a device after moving to a new Windows version, even if previously enabled. This ensures the admin has to consciously disable Microsoft's default protection from known issues for each new feature update.

Disabling safeguards does not guarantee your device will be able to successfully update. The update may still fail on the device and will likely result in a bad post-upgrade experience as you are bypassing the protection given by Microsoft pertaining to known issues. Only use this policy for testing purposes and not in production.

In the next section, you'll learn about options to deploy Windows updates faster.

Expediting a Windows patch

Expedited updates are a way to install Windows quality updates more quickly than normal. They can be useful when critical security events arise, and you need to deploy the latest updates more rapidly than normal.

With expedited updates, you can speed up the installation of quality updates like the most recent patch Tuesday release or an out-of-band security update for a zero-day flaw.

To speed up the installation, Windows Update is able to check for expedited updates more frequently than the normal Windows Update scan frequency. This process enables devices to start the downloading and installation of an expedited update as soon as possible, without having to wait for the device to check in for updates.

The actual time that a device starts to update depends on the device being online, its scan timing, whether communication channels to the device are functioning, and other factors like cloud-processing time.

Expedited updates override Windows Update for Business deferral policies so that the update is installed as quickly as possible. However, not all updates can be expedited. Currently, only Windows 10/11 security updates that can be expedited are available to deploy with the **Quality updates** policy.

By creating an expedite policy, the expectation is to get more than 90% of devices with an expedited policy assigned, updated, and restarted within 2 days. That also means that when using this type of policy, it can have a negative impact on your end users' productivity as it has a way more aggressive reboot behaviour.

Two to three times more devices are updated successfully in the first week of deployment compared to devices configured with Windows Update for Business ring policy settings.

One benefit of expediting an update is that you won't need to modify the existing quality update settings of your Windows 10 update rings. An expedited profile will temporarily override any Windows Update for Business settings and use the necessary settings from the expedited policy instead; this is to ensure the expedited update is installed as quickly as possible on the targeted devices. The settings from your Windows Update for Business policy will be automatically restored to the correct state after the expedited update is successfully installed.

Support for expediting an update policy is available on Windows 10 devices that are still receiving updates through Windows Update and have not reached the end of service. Devices need to be Hybrid Entra ID joined or Entra ID joined for the policy to work.

Expedited updates use **Windows Push Notification Services** (**WNS**) and push notification channels to deliver the message to devices that there's an expedited update to install. This is done to speed up installation. This process enables devices to start the download and install from Windows Update as an expedited update as soon as possible, without having to wait for the device to go through the normal scheduled check-in process for talking to the Windows Update backend service.

To expedite a Windows update, follow these steps:

1. In the Microsoft Intune admin center, go to **Devices | Windows | Quality updates for Windows 10 and later | Create profile**:

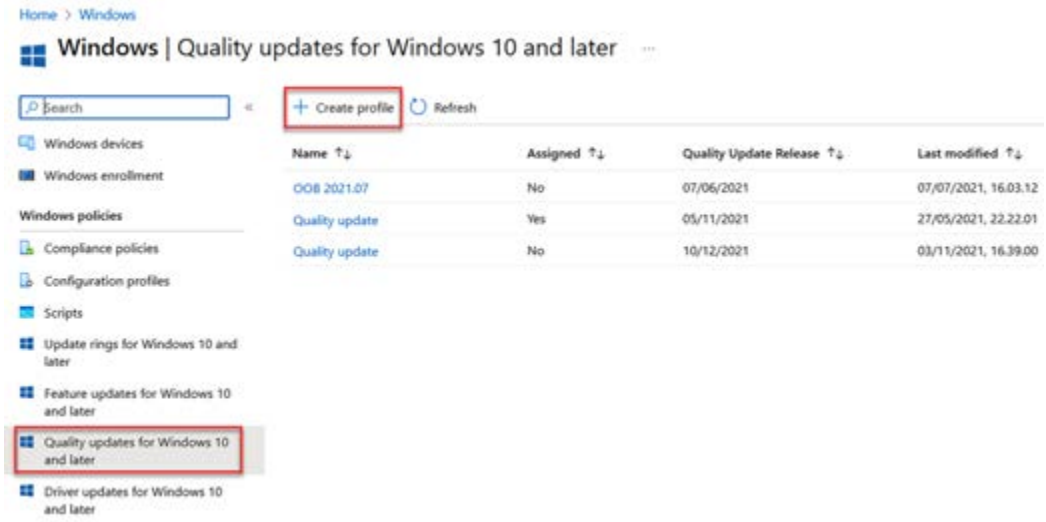


Figure 6.51: Quality updates for Windows 10 and later

2. You can select quality updates to be deployed. You can always select the three latest patches released for Windows:

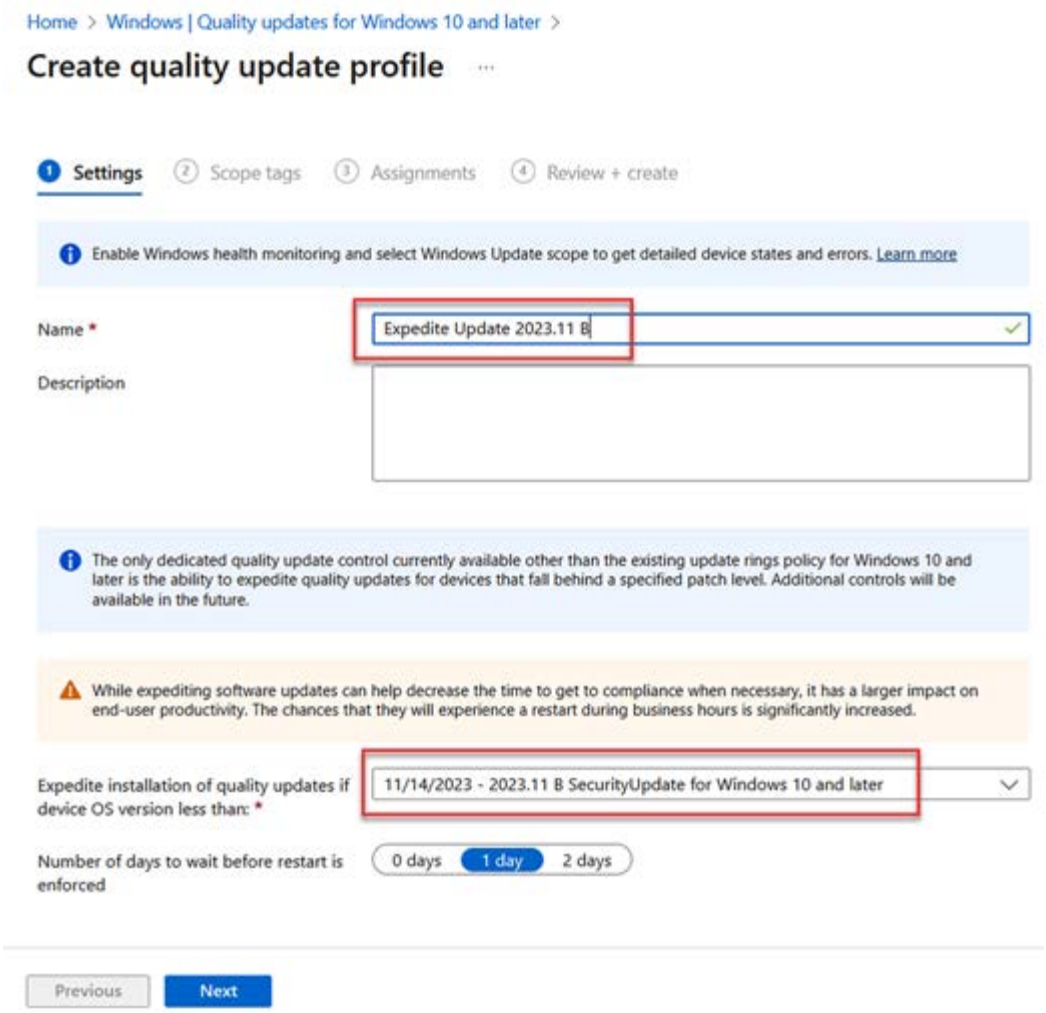


Figure 6.52: Quality updates for Windows 10 and later



IMPORTANT NOTE

Use **2 days** for the best end user experience. If the update is very important, select **0 days**, but be aware that the devices this policy is assigned to will force a reboot after the patch is downloaded and installed.

The following shows how the notifications keep getting more and more aggressive as the deadline approaches:

1. You will start by getting a message to restart in x days depending on the number of days set in the policy:



Figure 6.53: Restart in x days

2. Then, it will get more aggressive and show this message on the end user's screen 2 days before the restart, where the end user has the option to pick a time:

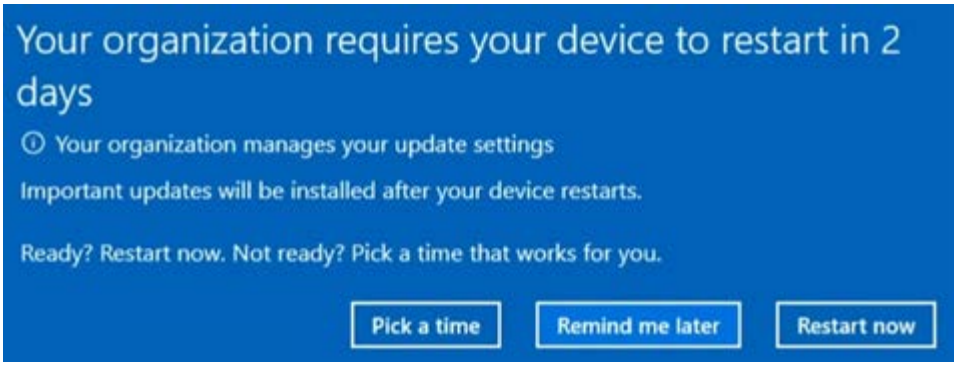


Figure 6.54: Notification to pick a time for restart

3. Then, it will get even more aggressive and show this message on the end user's screen 2 hours before the restart. The end user has the option to confirm and wait or restart now:

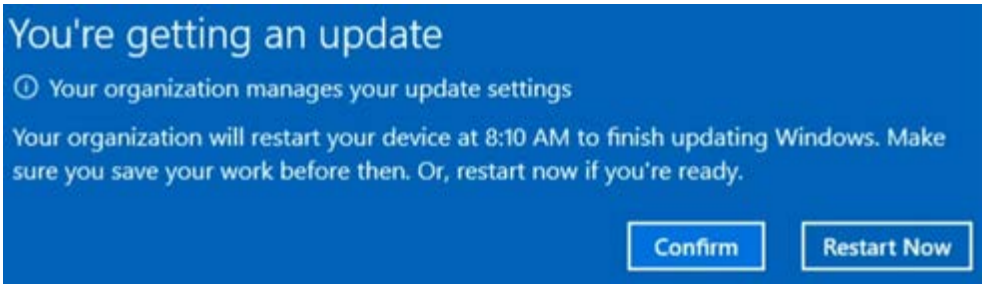


Figure 6.55: Notification 2 hours before restart

4. 15 minutes before the restart deadline, the end user only has the option to restart:



Figure 6.56: Forced restart

The Windows Insider Program for Business

As the IT admin, you can register your company's entire tenant at once for the Windows Insider Program for Business. The benefit of enrolling your corporate tenant for the Windows Insider Program for Business is that you, as an IT admin, can manage installations of Windows 10 and Windows 11 Insider Preview Builds across multiple devices in your organization using Microsoft Intune.

Register with either your Entra ID work account, which we recommend for the best experience, or your personal Microsoft account. If you use your organization's account, you'll be able to give Microsoft feedback on behalf of your organization to help shape Windows to meet your business's specific needs.

You must register with your Entra ID account to manage Windows 10/11 Insider preview builds centrally across your organization (`https://insider.windows.com/en-us/for-business`):

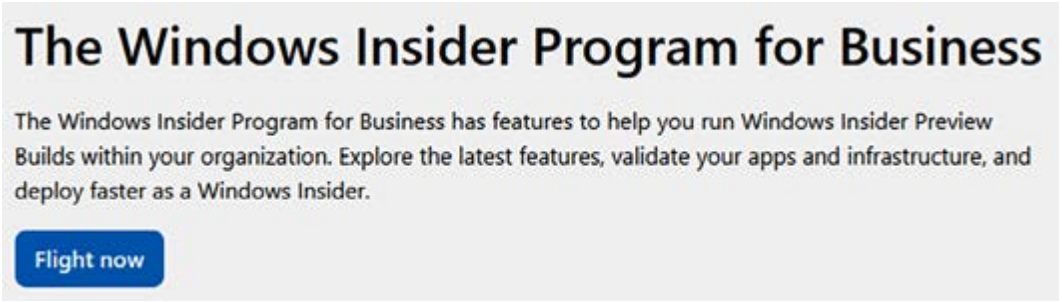


Figure 6.57: Windows Insider Program for Business

You need to register with your global admin account for Windows Insider for Business:



Figure 6.58: Windows Insider Program

You need to read the program agreement and click **I accept the terms of this agreement. (Required)** which will open the following screen:



Figure 6.59: Windows Insider Program welcome

Now your domain is registered to leverage Windows Insider for Business.

You can now create a Windows Update for Business ring deployment with Windows Insider rings and assign it to a group of test devices:

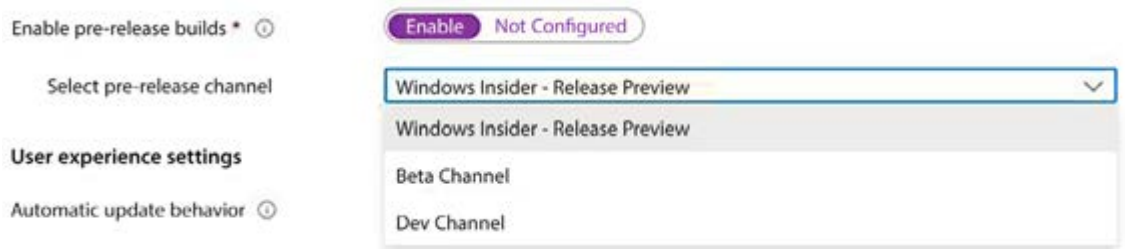


Figure 6.60: Windows Insider deployment ring

Your end users can now send feedback in Feedback Hub with their Entra ID account and other members of your organization can see this feedback. This is done as follows:

1. Select the **Feedback** section from the side menu in Feedback Hub.
2. Under the **Filter** dropdown, select **My organization.** This will show all the feedback from users in your organization who are also signed in to Feedback Hub using their registered Entra ID accounts:

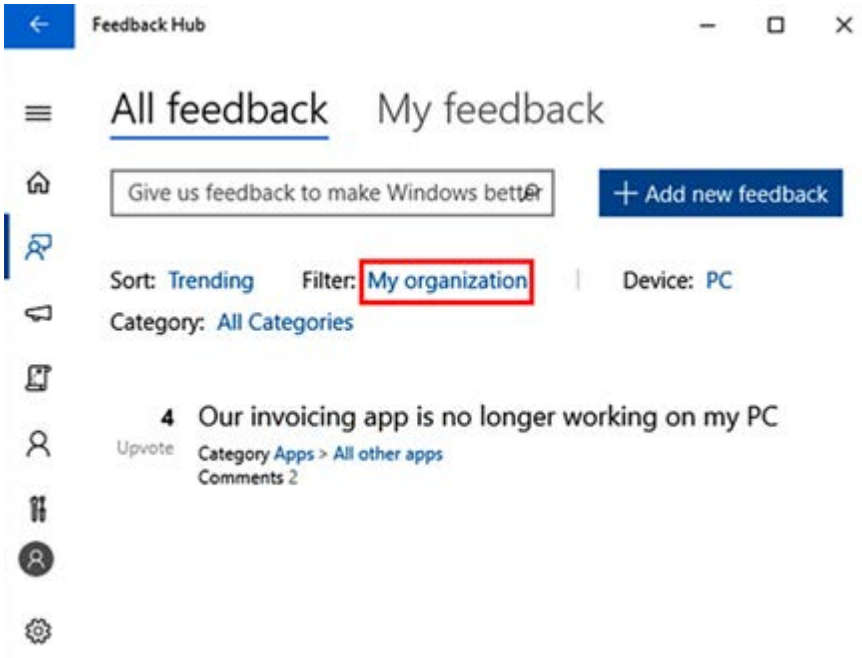


Figure 6.61: Windows Feedback Hub

Updating Microsoft 365 apps

When you start to leverage Windows Update for Business either on a cloud-managed device or a co-managed device, you should also look at how you are managing the updating of Microsoft 365 apps. We will now explain a couple of the options.

There are two options:

- **Servicing profile for Microsoft 365 apps:** You can see an overview of the devices in the **Servicing Profile** section of the Microsoft 365 apps admin center (`config.office.com`), including details on the next build rollout, projected waves, and information on any device failures and issues.

  From there, you can click on **Devices**, **Overview**, **Issues**, and **Settings** to get more information on devices managed by the servicing profile:



Figure 6.62: Microsoft 365 Apps Servicing Profile

- **Administrative templates to configure policies:** Administrative templates are the way that you are used to configuring policy settings in your on-premises environment with group policies.

This has brought us to the end of the chapter. We hope you enjoyed it!

The next section will be all about using Windows Update as a Service with Windows Autopatch.

Windows Autopatch

You'll learn about Windows Autopatch in this section. We explained in the first chapter that Windows Autopatch is a cloud-based solution that streamlines the update process for Windows, Microsoft 365 apps, Microsoft Edge, and Microsoft Teams. In this section, we will explain how you can enable this service inside your Microsoft Intune tenant settings.

Windows Autopatch requirements

Windows Autopatch is a cloud-based solution that streamlines the update process for Windows, Microsoft 365 applications, Microsoft Edge, and Microsoft Teams.

Your enterprise will need active Microsoft 365 E3/E5 licenses to use the service. The service leverages Windows Update for Business, among other components, to carry out updates on devices. Its primary objectives are to enhance security, boost productivity within organizations, and simplify the upkeep of digital infrastructure. Windows Autopatch was first announced in July 2022, and it was rolled out for general availability in November 2022.

How to enable Windows Autopatch



Before you continue, ensure that you have the required licenses for Windows Autopatch enabled inside your tenant.

To enable Windows Autopatch, go to **Tenant admininistration** | **Tenant enrollment** in the Intune Admin Center:

1. **Run checks** can help you to see whether you need to perform any steps before you can enable the service inside your tenant.

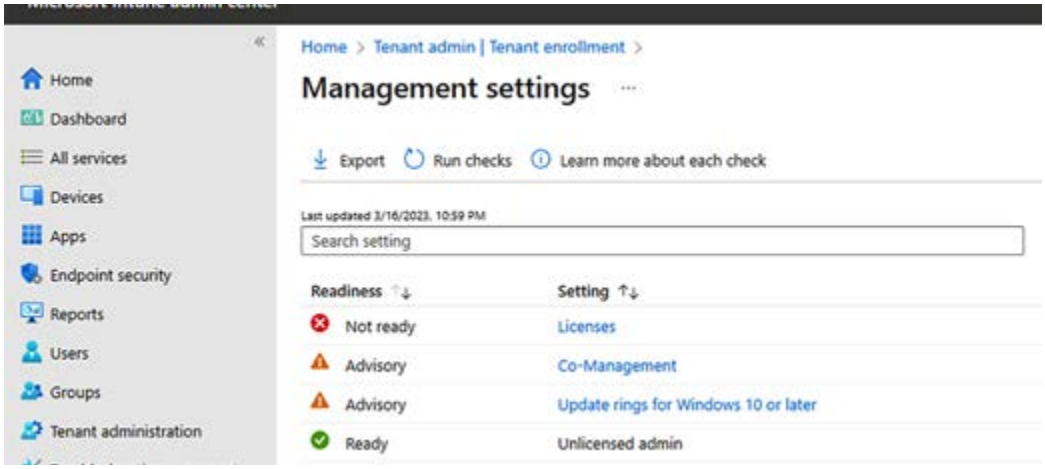


Figure 6.63: Windows Autopatch checks

2. **Enabling Windows Autopatch** is simple. If you have the proper licenses, you only need to **Agree** to the **terms** and **conditions**.

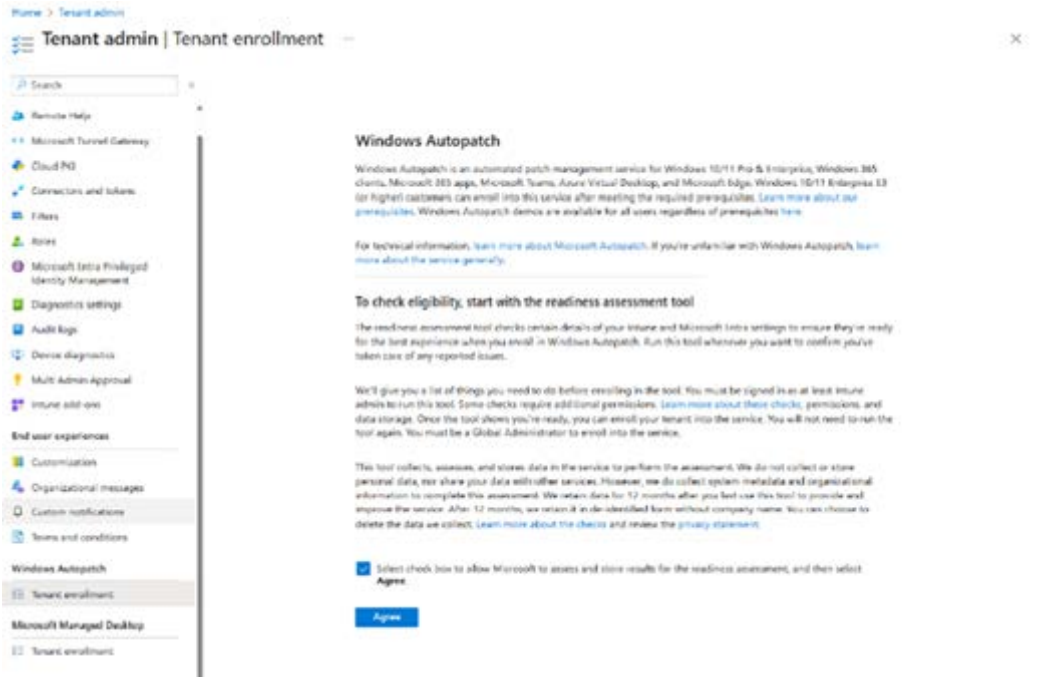


Figure 6.64: Windows Autopatch terms and conditions

3. When everything has run successfully, you can **start** the **enrollment** via the **Enroll** button.

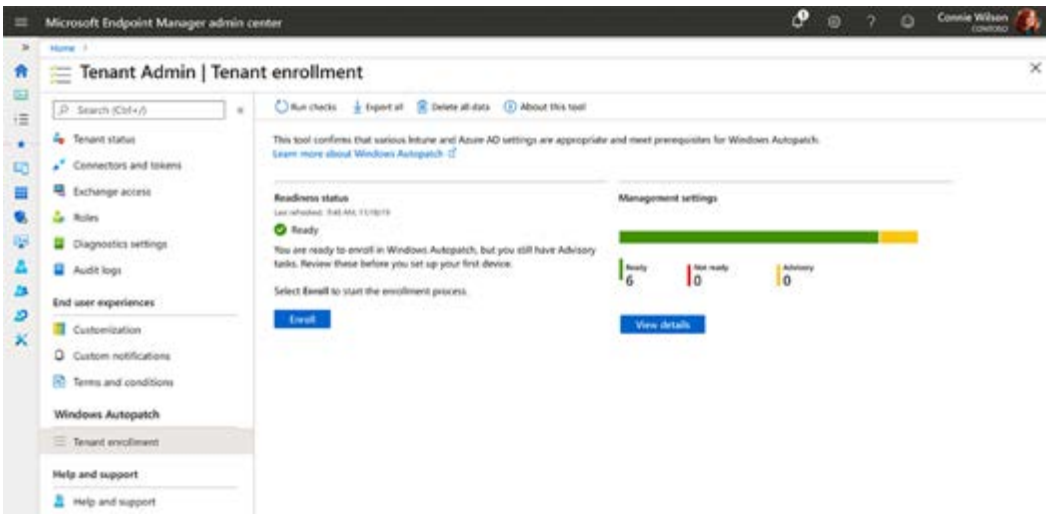


Figure 6.65: Enrolling into Windows Autopatch

4. As Autopatch is a managed service from Microsoft, you need to provide certain delegated permissions to Microsoft. Once you've agreed, click on **Agree**.

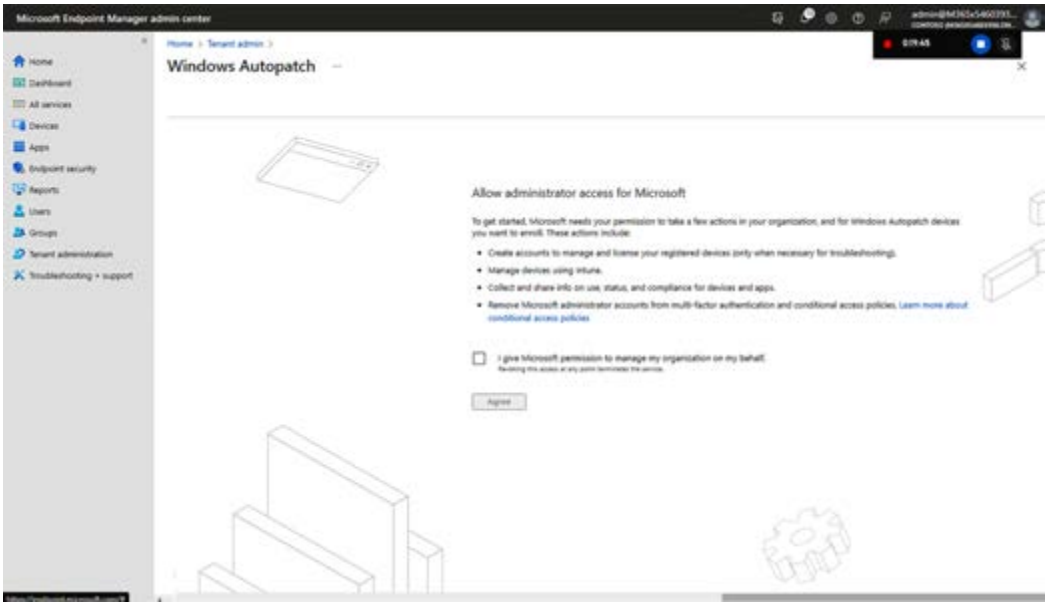


Figure 6.66: Delegating permissions to Microsoft

5. In case Microsoft needs to contact you about Windows Autopatch operational issues, provide your IT admin contact details. Once ready, hit **Complete**.

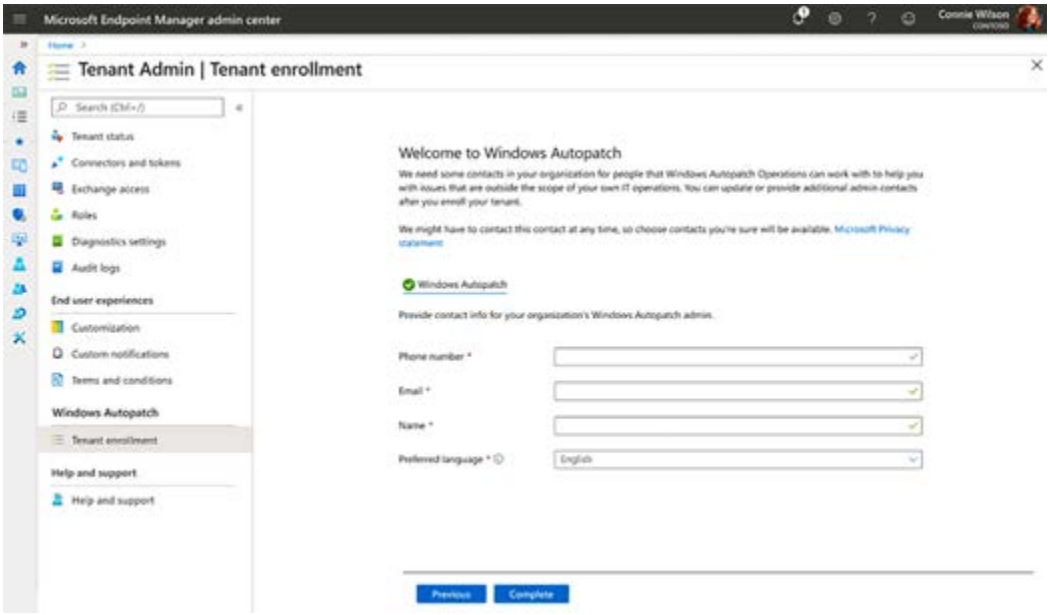


Figure 6.67: Providing IT admin contact details

6. Windows Autopatch creates a set of policies in your tenants that configures Windows Update settings, data collections related to Windows Update for Business and Windows Autopatch, and Office, Edge, and Teams update configuration policies:

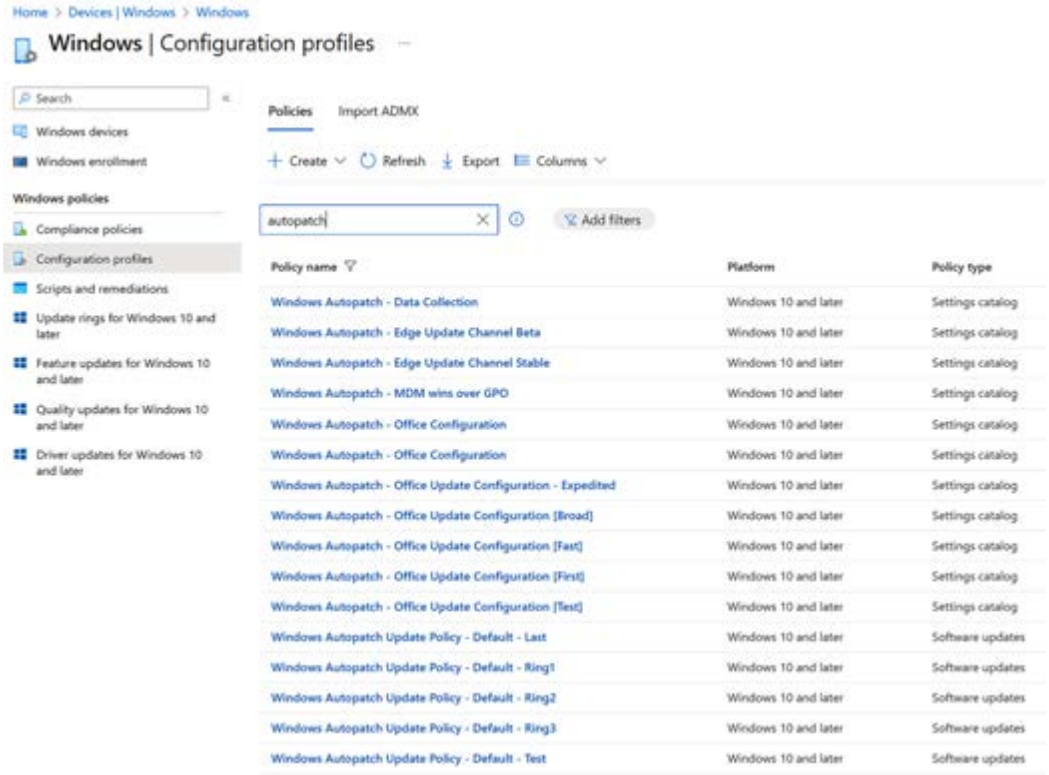


Figure 6.68: Windows Autopatch policies

Optimizing Windows Update rings

Windows Autopatch also allows us to set custom-scheduled Windows Update deployments for rings to groups of devices in separate rings to ensure the lowest-risk updates get pushed to the right set of people. Microsoft does recommend the default settings; we acknowledge that some organizations have unique needs.

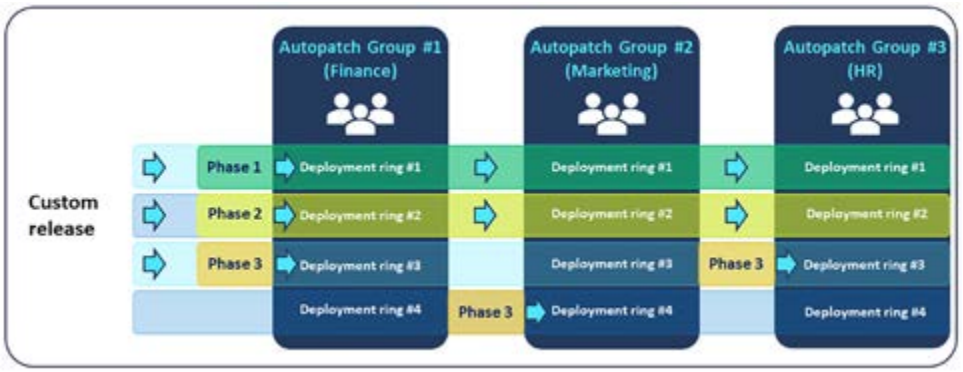


Figure 6.69: Windows Update rings and groups

In *Figure 6.69*, you can see how to configure rings and deployment cadences in Windows Autopatch. For example, you can configure deadline-driven updates to complete them at a scheduled time with a grace period to allow some extra flexibility.

Windows Autopatch automatically creates your deployment rings with the recommended settings; Autopatch creates five rings with corresponding Windows Update policies assigned to them.

Read more about the default Windows Update ring policy configuration here: `https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/deploy/windows-autopatch-groups-overview#default-update-deployment-cadences`

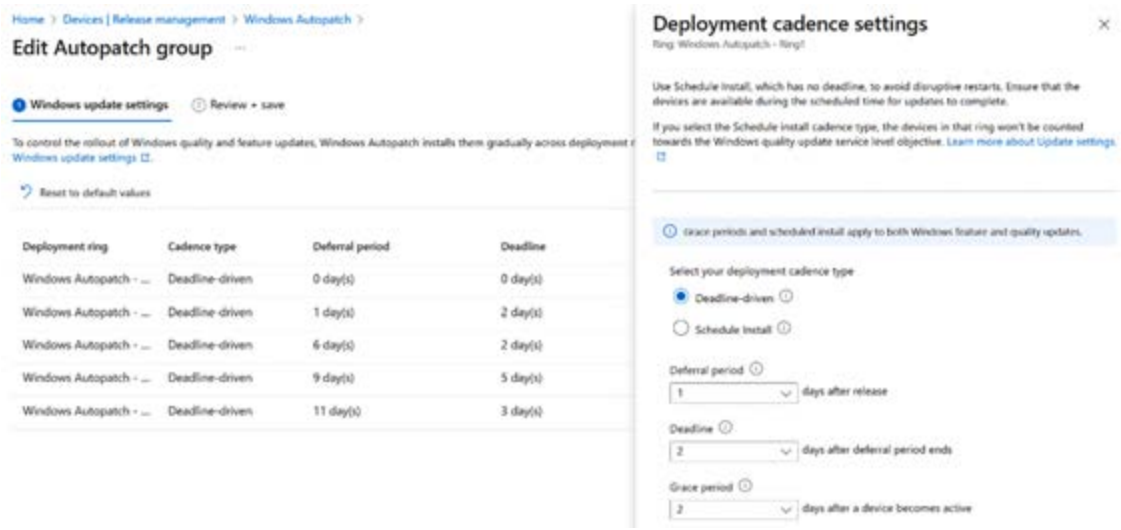


Figure 6.70: Customizing Windows Autopatch ring settings

Enabling Windows Autopatch for Cloud PCs

After configuring Windows Autopatch is complete, you can leverage the service within your Windows 365 Cloud PC provisioning policies.

Cloud PCs will automatically receive the necessary agents and configuration policies during provisioning to make your life much easier!

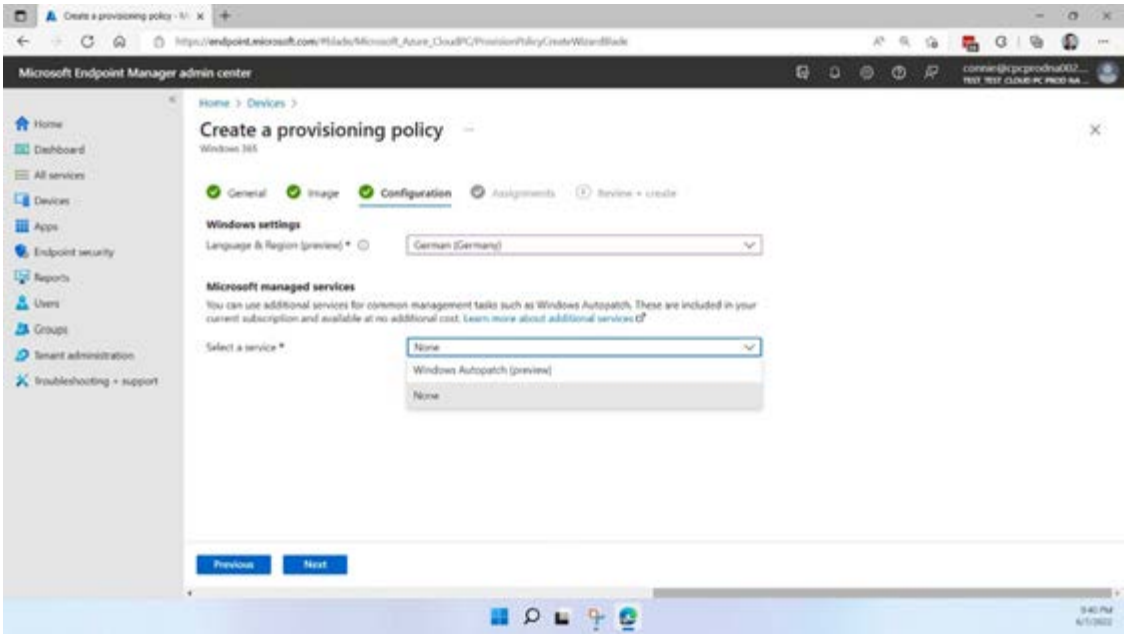


Figure 6.71: Enable Windows Autopatch in Windows 365 Enterprise

This has brought us to the end of the chapter. We hope you enjoyed it!

Summary

In this chapter, you've learned about all the things you need to know in order to start deploying and updating Windows using Microsoft Intune and Windows Update for Business for different endpoint scenarios.

We went through the different options on how to update Windows and what policy settings you should apply. If you are used to leveraging Microsoft Configuration Manager to handle Windows Update, you probably already have some kind of ring deployment for deploying Windows updates in your business. With servicing profiles in the Microsoft 365 Apps admin center, you can start taking a similar approach as Windows Update for Business has ring-based deployments as well.

If you are not already running Windows Autopatch or Windows Insider for Business, we explained why it is a good idea to start, and now you are ready to configure Windows Insider for Business in your organization for a select group of users or devices. In the next chapter, we're going to take a deeper dive into the world of Windows Autopilot.

Questions

1. What is Windows Update for Business?
    a. A way to update Microsoft apps
    b. A way to update Microsoft Edge
    c. A way to update Windows
2. What is the maximum number of days that can be configured for the **Set feature update uninstall period** option?
    a. 30
    b. 60
    c. 90
3. Which license do you need for Windows Autopatch?
    a. EMS
    b. Windows 365
    c. Windows E3

Answers

1. (c)
2. (b)
3. (c)

Further reading

If you want to learn more about the Microsoft Intune requirements after reading this chapter, please use one of the free online resources listed here:

- Learn about using Windows Update for Business, Microsoft docs: `https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure`
- Understanding hybrid Azure AD join and co-management: `https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/understanding-hybrid-azure-ad-join-and-co-management/ba-p/2221201`

Join the CloudPro Newsletter with 44000+ Subscribers

Want to know what's happening in cloud computing, DevOps, IT administration, networking, and more? Scan the QR code to subscribe to **CloudPro**, our weekly newsletter for 44,000+ tech professionals who want to stay informed and ahead of the curve.



`https://packt.link/cloudpro`

7

Windows Autopilot

In this chapter, you will learn about Windows Autopilot, including how it works, why it could be beneficial for your organization, and how it simplifies the delivery process of your physical endpoints.

Windows Autopilot is a collection of technologies used to preconfigure brand-new devices and get them into a state to enable the end user to be productive. Windows Autopilot is designed to easily onboard a brand-new device from anywhere. Previously, enterprises relied on **Operating System Deployment** (**OSD**) but, during the global COVID pandemic, where many employees were working from home, more and more enterprises looked for alternatives to get new devices to their end users even when working from home. Windows Autopilot is a perfect fit for this scenario, where an **Original Equipment Manufacturer** (**OEM**) or reseller can send the device directly to the end user, who can then unbox the new device, get it up and running, and start working without any need to go into the office.

In this chapter, we'll go through the following topics:

- Windows Autopilot overview
- Uploading the hardware ID to Windows Autopilot
- Windows Autopilot for existing devices
- Windows updates during the **Out-of-Box Experience** (**OOBE**)
- **Enrollment Status Page** (**ESP**)
- Autopilot reporting and diagnostics
- Cloud configuration scenario
- Edge kiosk self-deployment scenario
- Wiping and resetting your devices
- Fresh start

Technical requirements

Windows Autopilot has some prerequisites:

- **Microsoft Entra ID** automatic enrollment needs to be configured.

- The user needs an Intune license.
- The device needs to be registered in the Windows Autopilot service.
- Entra ID branding needs to be configured.

Windows Autopilot overview

Windows Autopilot is a provisioning method for modern devices. It is not OSD in the traditional manner. Windows Autopilot requires a cloud identity and cloud device identity, which can be either a *hybrid Entra ID join* or an *Entra ID join*. In this book, we will only cover *Windows Autopilot with Entra ID-joined devices*, as this is the cloud-native solution recommended by Microsoft when talking about brand-new devices.

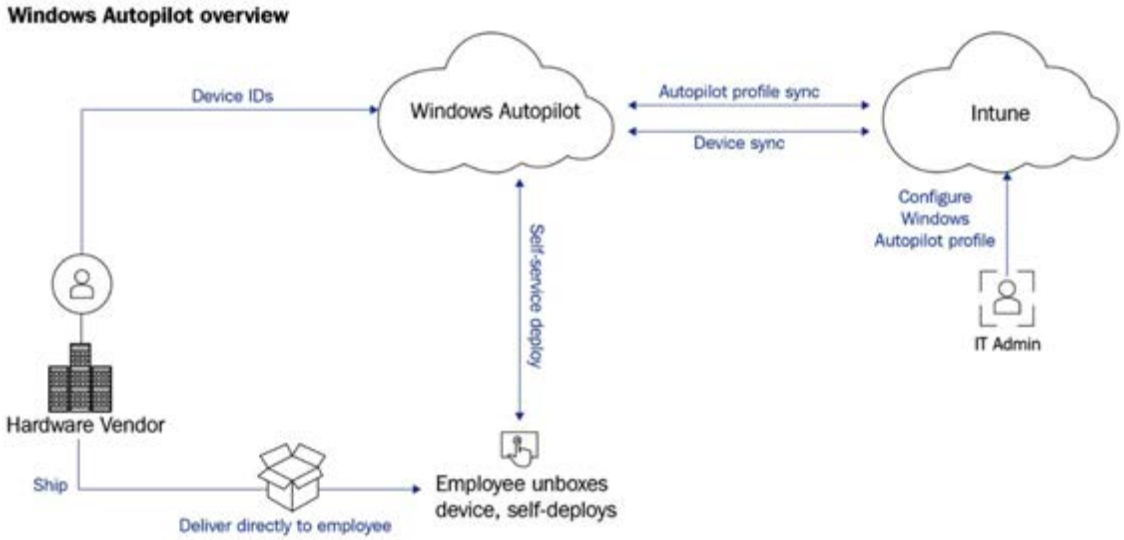


Figure 7.1: Autopilot process

You get started with Autopilot by getting your devices uploaded to the Autopilot service, creating and assigning an Autopilot profile, and then creating and assigning an ESP profile (this step is optional but recommended).

After your device is shipped, the user simply has to enter their credentials before automatic enrollment starts. It is as simple as that.

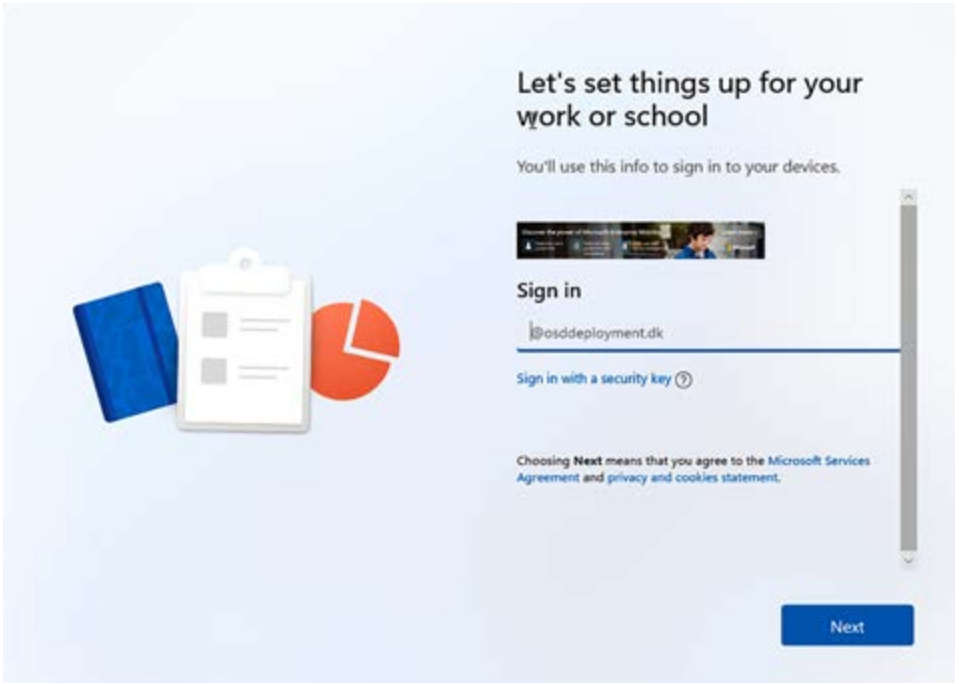


Figure 7.2: Autopilot welcome screen

After entering the correct credentials, you will be met by the Entra ID sign-in workflow.

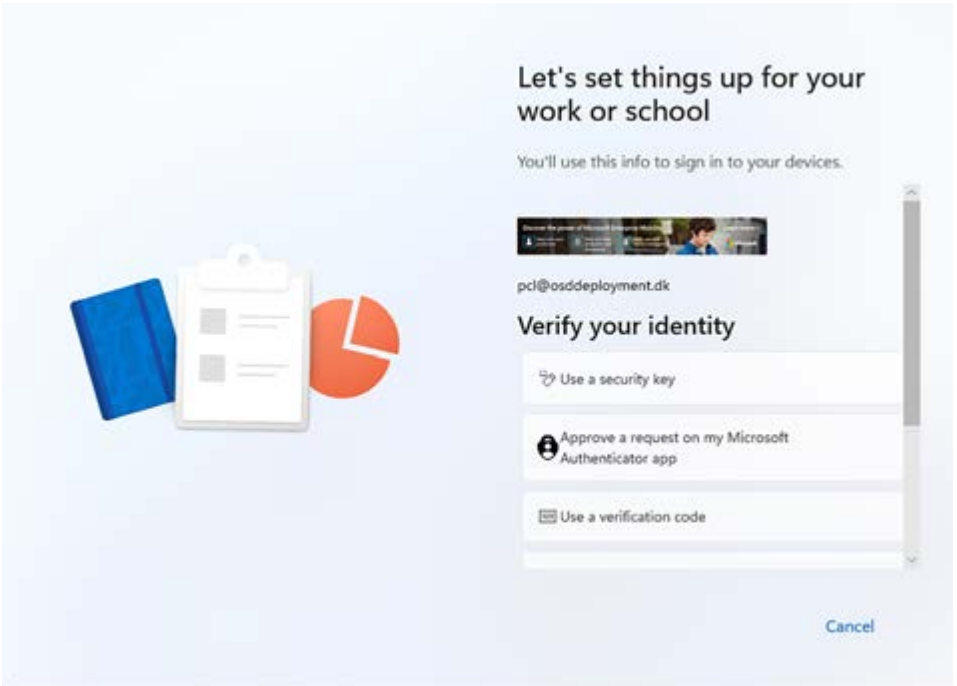


Figure 7.3: Verify your identity

Then, enrollment starts, and all your configuration items, policies, certificates, and applications are applied to your physical endpoint device.

As soon as this phase is completed, the user can see the desktop:

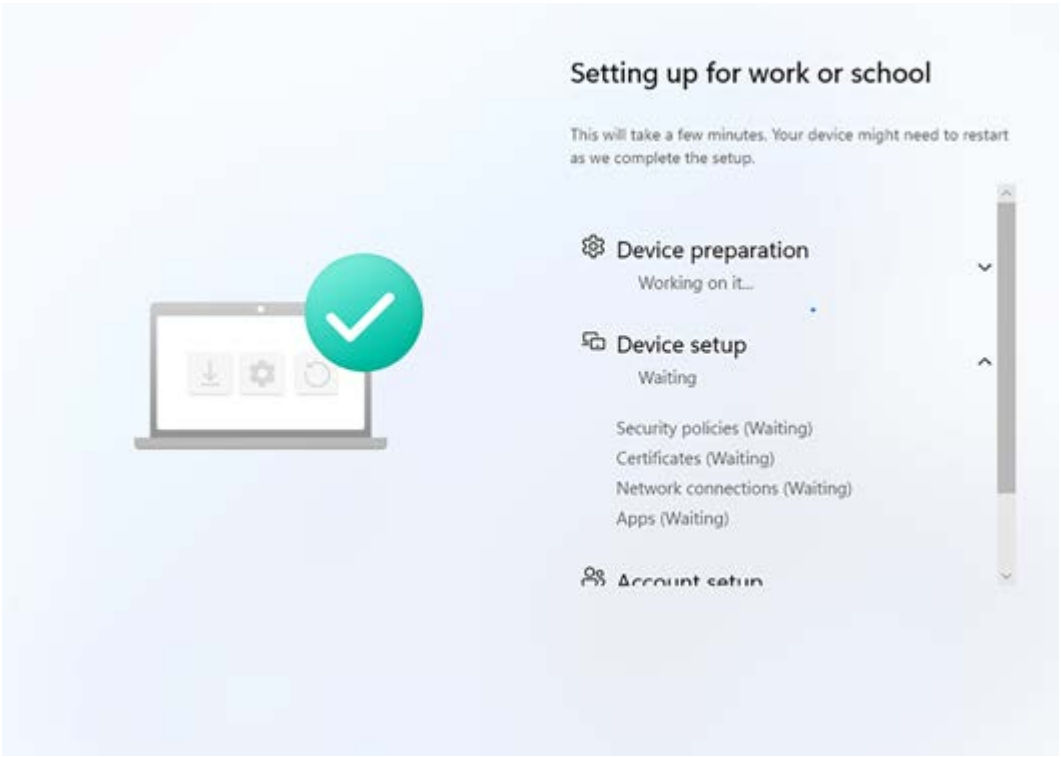


Figure 7.4: Autopilot device setup

If you use Enterprise State Roaming and OneDrive for Business known folder move, you will experience a familiar desktop environment, as most components of your profile will be synchronized from the cloud to your device.

In the next section, we're going to explain how you can add your devices to Windows Autopilot with the hardware ID as a unique indicator.

Uploading the hardware ID to Windows Autopilot

The Windows Autopilot hardware hash is a 4K string retrieved from the Windows 10 or Windows 11 OS on the device by running `Get-WindowsAutoPilotInfo.ps1` from a PowerShell prompt:

```
New-Item -Type Directory -Path "C:\Temp\Autopilot"
Set-Location -Path "C:\Temp\Autopilot"
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted
Install-Script -Name Get-WindowsAutoPilotInfo
Get-WindowsAutoPilotInfo.ps1 -OutputFile AutoPilotHWID.csv
```

Windows Autopilot device registration can be done within your organization manually, for testing, or for devices your organization already owns.

It is used to collect the hardware identity of devices (hardware hashes) and upload this information in a **Comma-Separated Values** (**CSV**) file to the Windows Autopilot service from the Microsoft Intune admin center, and also to capture the hardware hash for manual registration, which requires booting the device into Windows 10 or Windows 11. Therefore, this process is intended primarily for testing and evaluation scenarios. When having the OEM upload the devices into the Windows Autopilot service, you (as an IT admin) do not need to unbox and collect the hardware hash yourself.

The recommended way to get your brand-new devices into the Windows Autopilot service is to have your OEM or a Microsoft **Cloud Solution Provider** (**CSP**) partner upload the information.

For *Microsoft Surface* or *HoloLens 2* devices, you can open a support case with Microsoft Devices Autopilot Support: `https://learn.microsoft.com/en-us/surface/surface-autopilot-registration-support`. You only need to provide the following information:

- Entra ID tenant ID
- Entra ID domain name
- Proof of ownership
- Device serial numbers

This process can also be used to deregister Autopilot from your tenant.

You can have a CSP partner upload your devices into Windows Autopilot with very little information compared to when you do it yourself in Microsoft Intune:

- `ProductKey` only
- `SerialNumber` + `OemManufacturerName` + `ModelName`

Let's describe each of these fields:

- `ProductKey`: This is the Windows product ID – that is, the `Product Key ID`(`PKID`), a 13-digit number that corresponds to the Windows product key that was inserted into the firmware of the device at the time of manufacture (using `OAv3`).
- `SerialNumber`: This is the unique value assigned by the OEM to each device manufactured.
- `OemManufacturerName`: This is the value specified by the OEM in the **System Management Basic Input/Output System** (**SMBIOS**) firmware of the device – for example, *Microsoft Corporation or Lenovo* (more on that later).
- `ModelName`: This is the value specified by the OEM in the SMBIOS firmware of the device for the particular model – for example, *Surface Pro 7*.

You can have up to 500 rows in the CSV file. The header and line format are shown next, which include the device serial number, the Windows product ID, the hardware hash, the group tag, and the assigned user:

```
<serialNumber>,<ProductID>,<hardwareHash>,<optionalGroupTag>,<optionalAssignedUser>
```



Import Windows Autopilot devices from a CSV file. When assigning users in the CSV file, make sure that you are assigning the correct **User Principal Name** (**UPN**) as there is no validation of UPNs during the import process. This means that if an incorrect UPN is in the CSV file, the target user will not be assigned to the Windows Autopilot device object.

Assigning a user to a specific Autopilot device does not work if you are using **Active Directory Federation Services** (**ADFS**).

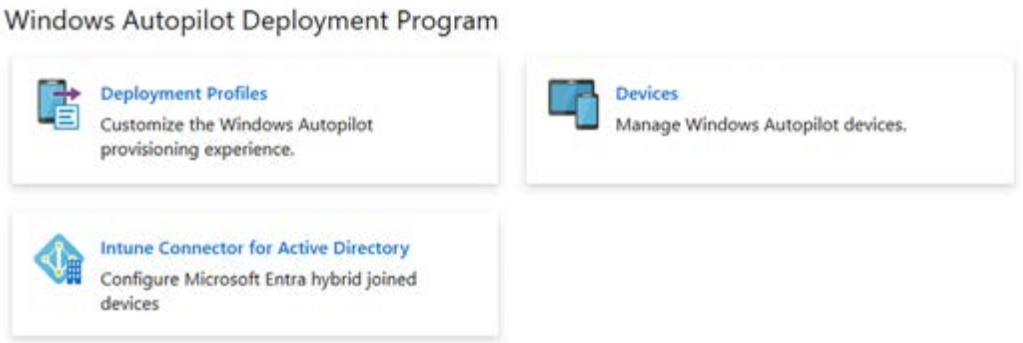


Figure 7.5: Windows Autopilot Deployment Program

To import Autopilot device IDs, follow these steps:

1. In the Microsoft Intune admin center, go to **Devices** | **Windows** | **Windows enrollment** | **Devices** and click **Import**:

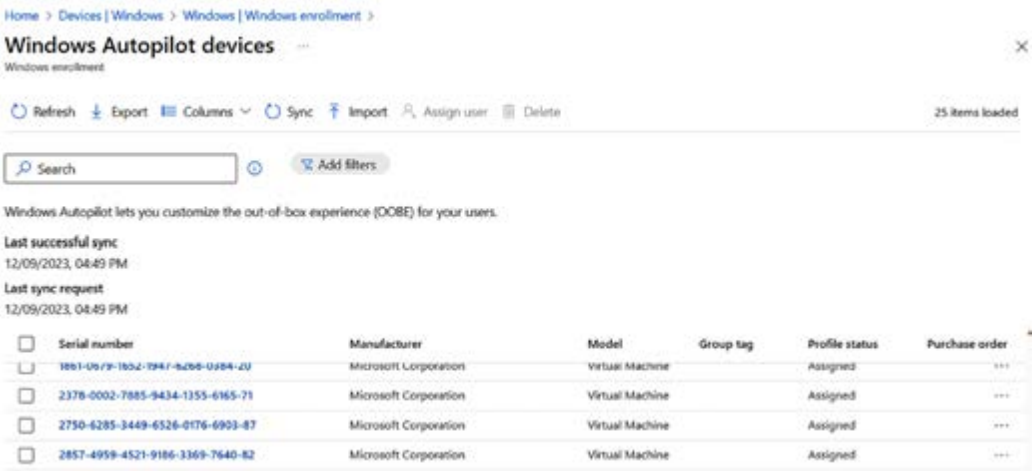


Figure 7.6: Windows Autopilot devices

2. Browse for your `autopilot.csv` file and then choose **Import**.

3. You will get the following message in the portal: **Import in progress. Elapsed time: 0 min.** This process can take up to 15 minutes.

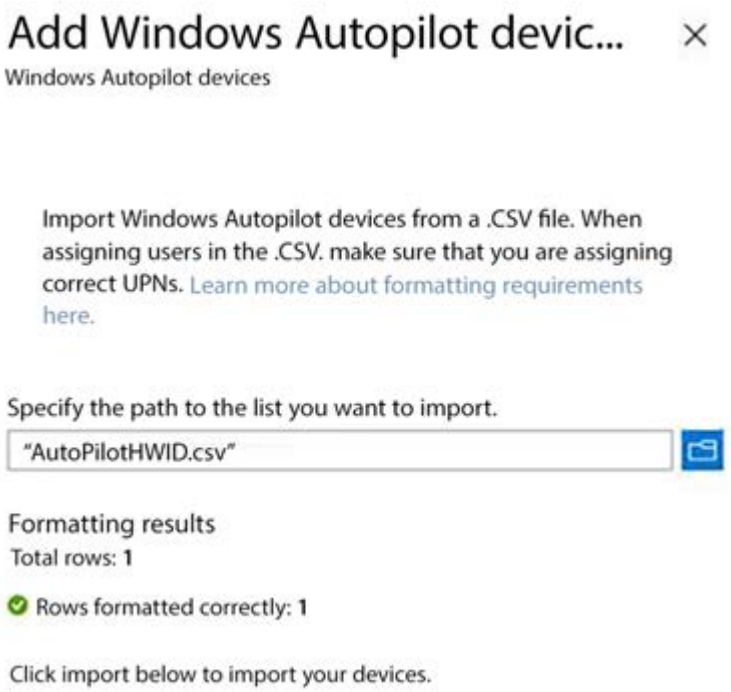


Figure 7.7: Add Windows Autopilot devices

4. Select a device. Choose **Assign user**.
5. Browse for your user and select the user you want to assign to the device:

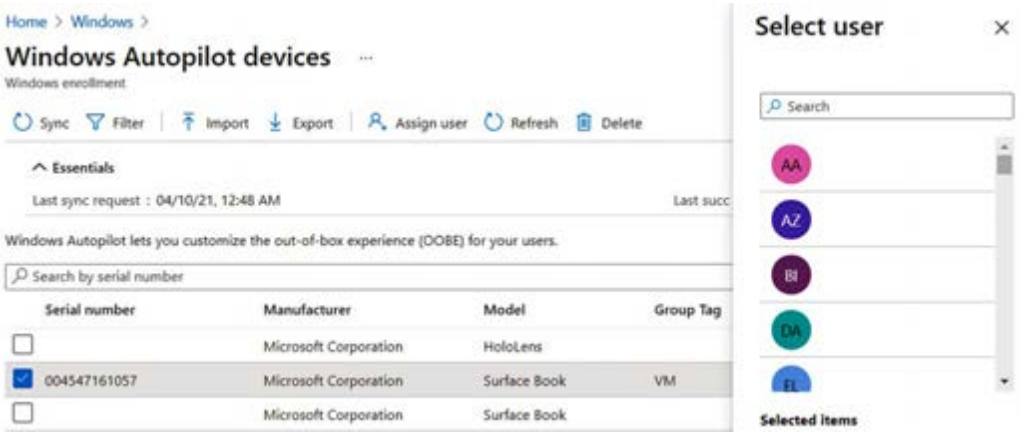


Figure 7.8: Assign user

When you are selecting a device in the **Windows Autopilot devices** blade, you will get some more information and some attributes that can be changed as an IT admin:



Figure 7.9: Windows Autopilot devices

In the following table, you can see the different types of settings and values that can be present in a Windows Autopilot object:

Setting	Value
User	UPN
User Friendly Name	Can be changed and it will be shown during OOBE provisioning
Serial number	Serial number
Manufacturer	Example: “Microsoft Corporation.”
Model	Example: “Surface Book 2.”
Device Name	Can be configured and the device will get this name as part of the onboarding process (will cause a reboot while the device name is being set during OOBE).
Group Tag	Blank unless it is set to the autopilot upload file. Can be changed and will affect a dynamix AAD group.
Profile status	Assigned or not assigned.
Assigned profile	Name of the profile assigned to the device.
Date assigned	Timestamp of when the profile was assigned to the device.
Enrollment state	Specifies whether the device has enrolled in Microsoft Intune. **Enrolled** or **Not enrolled**.
Associated Intune device	N/A means that there’s no associated device. N/A is the state until the device has gone throught the Autopilot process for the first time, or the Intune object has been deleted.
Associated Azure AD device	N/A means that there’s no associated device AAD object.
Last contacted	Timestamp of when the device was last contacted. Doesn’t mean that the device has never been in contact with Microsoft Intune.
Purchase order	Purchase order ID is sent from the OEM when they are uploading devices on behalf of your organization.

Table 7.1: Windows Autopilot object settings

You can also search for your devices once they are imported into the Autopilot service – including adding a filter that makes it easier to search for specific devices.

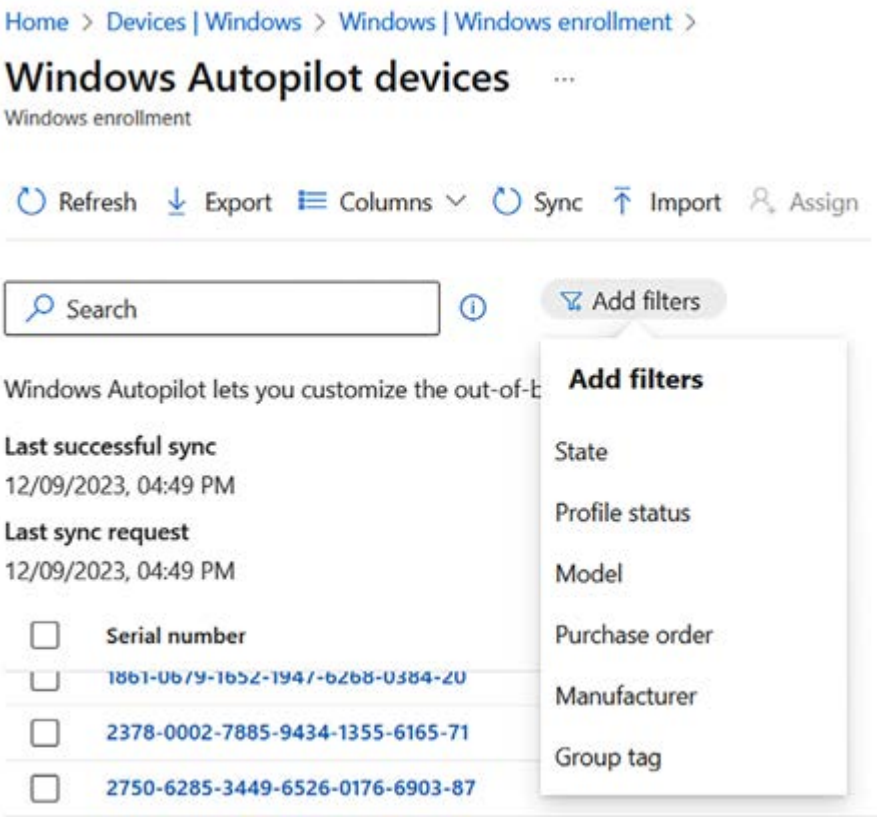


Figure 7.10: Windows Autopilot Add filters

Newer Windows versions have a 4K hardware hash that is used in the Windows Autopilot service. Examples include where a new hardware hash is needed if the **Trusted Platform Module** (**TPM**) or motherboard is replaced. The ways that a device is known in the Windows Autopilot service are based on the SMBIOS UUID, **Media Access Control** (**MAC**), or the disk serial number – the reason for this is that there is no unique identifier for a Windows device. If we look at what information is contained in the Autopilot hardware hash, then we also get an idea of why we need a new hardware hash following a motherboard replacement.

The minimum requirements for unique values in the SMBIOS are as follows:

- `ProductKeyID`
- `SmbiosSystemManufacturer`
- `SmbiosSystemProductName`
- `SmbiosSystemSerialNumber`
- `SmbiosSkuNumber`
- `SmbiosSystemFamily`

- `MacAddress`
- `SmbiosUuid`
- `DiskSerialNumber`
- `TPM EkPub`

Where is Windows Autopilot device information stored?

Windows Autopilot data is stored within the **European Union** (**EU**), and not in the region where your Entra ID tenant is located. It is not customer data that is stored, but business data, which enables Microsoft to provide the Windows Autopilot service, and customers can always opt out of the Windows Autopilot service.

If you want to want to learn more about what the Windows Autopilot hardware hash contains, you can find out from the following steps.

First, you need to download the Windows **Assessment and Deployment Kit** (**ADK**) from `https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install`:

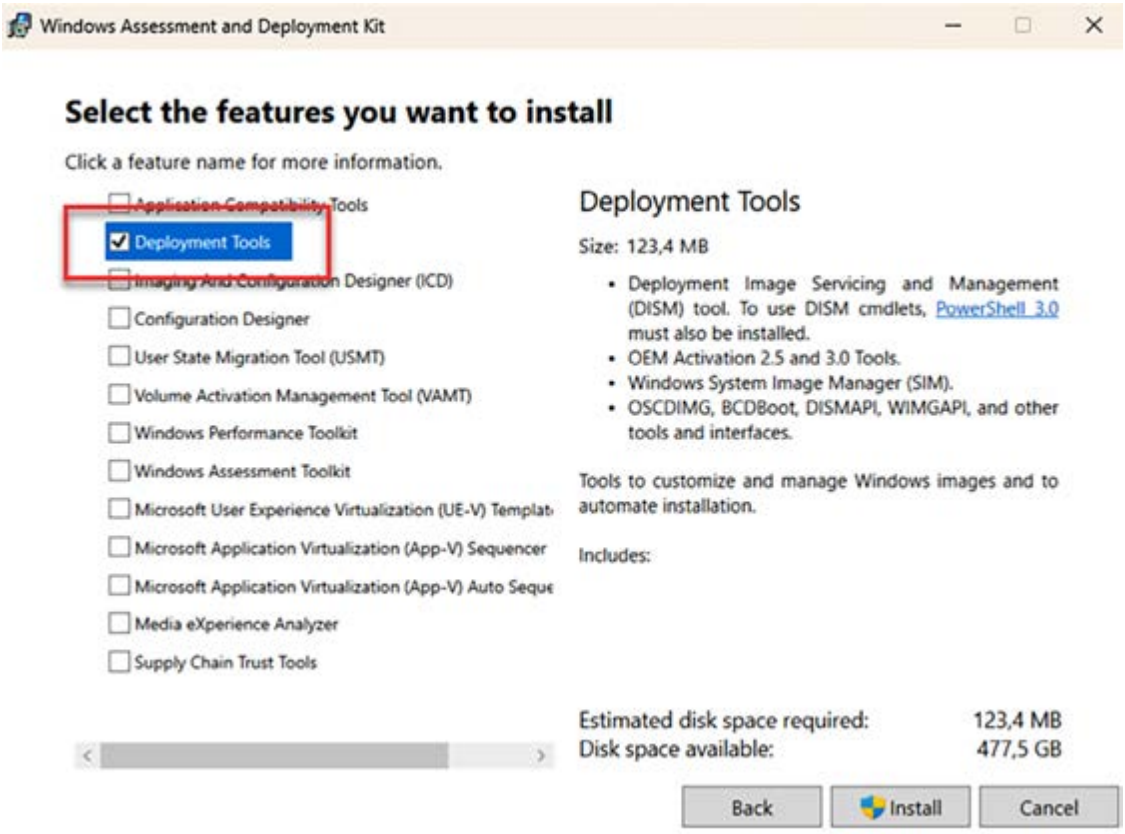


Figure 7.11: Windows ADK

Following the installation of the Windows ADK, you can find the tool you need here:

```
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment
Tools\amd64\Licensing\OA30\oa3tool.exe
```

Say you run the following command:

```
oa3tool.exe /DecodeHwHash=HardwareHash
```

Then, you'll get the decoded result of what is stored in the hardware hash:

```
OEM Activation Tool 3.0
(c) Copyright 2023 Microsoft Corp.

Version: 10.0.25398.
<?xml version="1.0"?>
<HardwareReport>
     <HardwareInventory>
           <p n="ToolVersion" v="3" />
           <p n="HardwareInventoryVersion" v="131" />
           <p n="ToolBuild" v="10.0.17134.1" />
           <p n="OSType" v="FullOS" />
           <p n="OsCpuArchitecture" v="x64" />
           <p n="OsBuild" v="10.0.17134.1" />
           <p n="OsSystemTime" v="2018-05-18T12:51:13Z" />
           <p n="OsLocalTime" v="2018-05-19T18:51:13+30:00" />
           <p n="ProcessorModel" v="     Intel(R) Xeon(R) CPU E3-1220L V2 @
2.30GHz" />
           <p n="ProcessorPackages" v="1" />
           <p n="ProcessorThreads" v="2" />
           <p n="ProcessorCores" v="2" />
           <p n="ProcessorHyperThreading" v="false" />
           <p n="SmbiosRamArrayCount" v="1" />
           <p n="SmbiosRamSlots" v="1" />
           <p n="SmbiosRamErrorCorrection" v="None" />
           <p n="SmbiosRamMaximumCapacity" v="2048" />
           <p n="TotalPhysicalRAM" v="2" />
           <p n="SmbiosFirmwareVendor" v="Microsoft Corporation" />
           <p n="SmbiosSystemManufacturer" v="Microsoft Corporation" />
           <p n="SmbiosSystemProductName" v="Virtual Machine" />
           <p n="SmbiosSystemSerialNumber" v="2378-0002-7885-9434-1355-6165-71"
/>
           <p n="SmbiosUuid" v="192a7ab2-4b1d-4433-9026-3b54c6e8353c" />
           <p n="SmbiosSkuNumber" v="None" />
```

```
            <p n="SmbiosSystemFamily" v="Virtual Machine" />
            <p n="SmbiosSystemVersion" v="Hyper-V UEFI Release v1.0" />
            <p n="SmbiosBoardManufacturer" v="Microsoft Corporation" />
            <p n="SmbiosBoardProduct" v="Virtual Machine" />
            <p n="SmbiosBoardVersion" v="Hyper-V UEFI Release v1.0" />
            <p n="ChassisType" v="0x03" />
            <p n="Disk1.DiskCapacity" v="80" />
            <p n="Disk1.DiskType" v="HDD" />
            <p n="Disk1.StorageBusType" v="SAS" />
            <p n="Disk1.IncursSeekPenalty" v="255" />
            <p n="Disk1.TrimEnabled" v="1" />
            <p n="Disk1.DiskSerialNumber" v="|Virtual Disk    |Msft    " />
            <p n="InternalDiskCount" v="1" />
            <p n="TotalDiskCapacity" v="80" />
            <p n="OpticalDiskDriveType" v="true" />
            <p n="PhysicalMedium" v="Unspecified" />
            <p n="MacAddress" v="00:15:5D:00:0A:49" />
            <p n="DisplayResolutionHorizontal" v="1024" />
            <p n="DisplayResolutionVertical" v="768" />
            <p n="DisplaySizePhysicalH" v="0" />
            <p n="DisplaySizePhysicalY " v="0" />
            <p n="DigitizerSupportID" v="(null)" />
            <p n="PowerPlatformRole" v="Desktop" />
            <p n="Status" v="0x00000000" />
            <p n="OfflineDeviceIdType" v="UEFI_VARIABLE_RANDOMSEED" />
            <p n="OfflineDeviceId"
v="deabBSuZ84Ttjnd+ipi2q9gwdtwBUrOYwUmzOEOnbYo=" />
            <p n="DiskSSNKernel" v="|Virtual Disk    |Msft    " />
     </HardwareInventory>
</HardwareReport>
```

The OEM activation tool 3.0 successfully completed its required processes.

Windows Autopilot for existing devices

If you do not want to collect and upload the devices into Autopilot, some other options are available to you.

For devices already in Intune, which can be Entra ID-joined devices or co-managed devices, you can leverage **Convert all targeted devices to Autopilot** in the Autopilot profile:

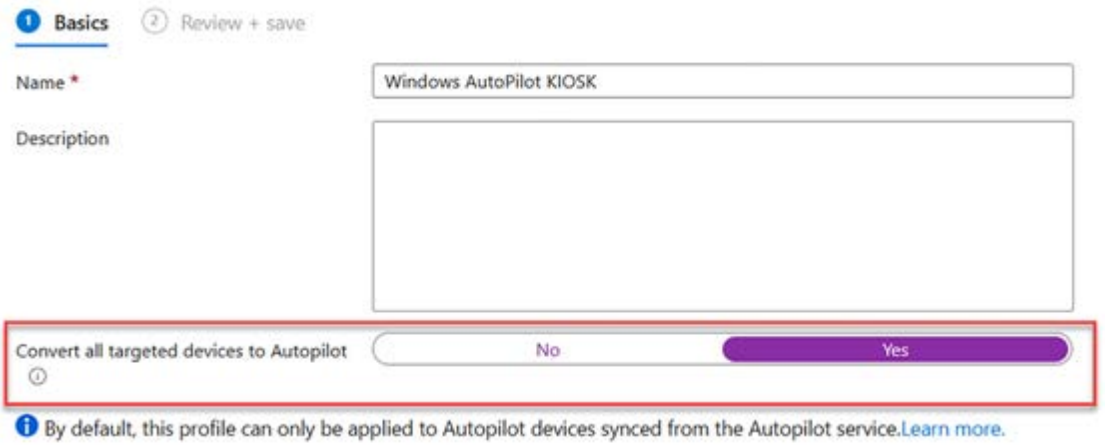


Figure 7.12: Convert all targeted devices to Autopilot

Select **Yes** to register all targeted devices to Autopilot if they are not already registered. The next time registered devices go through the Windows OOBE, they will go through the assigned Autopilot scenario.

Using the **Convert all targeted devices to Autopilot** setting doesn't automatically convert existing Microsoft Entra hybrid devices in the assigned group(s) into a Microsoft Entra device. The setting only registers the devices in the assigned group(s) for the Autopilot service.

Removing this profile won't remove affected devices from Autopilot. To remove a device from Autopilot, use the **Windows Autopilot devices** view.

You can also leverage Windows Autopilot for existing devices by doing traditional OS deployment from **System Center Configuration Manager** (**SCCM**) or the **Microsoft Deployment Toolkit** (**MDT**).

All you need to do is to put the Autopilot profile in `%windir%\provisioning\AutoPilot\AutopilotConfigurationFile.json`.

You need to have administrator rights on the Windows device you are running this from.

When you have created an Autopilot profile in Microsoft Intune, you can export it by leveraging the **WindowsAutopilotIntune** PowerShell module:

```
Install-Module WindowsAutopilotIntune -Force
Install-Module Microsoft.Graph.Intune -Force
Connect-MgGraph
Get-Autopilotprofile
```

You will get a list of all Autopilot profiles in your tenant. The following is an example. Now you can leverage the ID to get it and convert it to the required JSON content:

```
@odata.type                    : #microsoft.graph.
azureADWindowsAutopilotDeploymentProfile
id                             : 264c05b0-683c-4537-87ff-1ff5151d5b98
displayName                    : Intune Book
description                    :
language                       : os-default
createdDateTime                : 4/10/2023 9:59:13 AM
lastModifiedDateTime           : 4/10/2023 9:59:13 AM
enrollmentStatusScreenSettings :
extractHardwareHash            : True
deviceNameTemplate             : OSD-%RAND:5%
deviceType                     : windowsPc
enableWhiteGlove               : True
roleScopeTagIds                : {0}
outOfBoxExperienceSettings     : @{hidePrivacySettings=True; hideEULA=True;
userType=standard; deviceUsageType=singleUser;
                                 skipKeyboardSelectionPage=True;
hideEscapeLink=True}
```

When you are calling the command with the unique Autopilot profile ID, you can convert it to the JSON file you need on the Windows device during the image process:

```
Get-Autopilotprofile -id 264c05b0-683c-4537-87ff-1ff5151d5b98 | ConvertTo-
AutopilotconfigurationJSON
{
    "CloudAssignedDomainJoinMethod":  0,
    "CloudAssignedDeviceName":  "OSD-%RAND:5%",
    "CloudAssignedAutopilotUpdateTimeout":  1800000,
    "CloudAssignedForcedEnrollment":  1,
    "Version":  2049,
    "CloudAssignedTenantId":  "c56dd45b-1da6-4bd0-a53b-1466782d6ee5",
    "CloudAssignedAutopilotUpdateDisabled":  1,
    "ZtdCorrelationId":  "264c05b0-683c-4537-87ff-1ff5151d5b98",
    "Comment_File":  "Profile Intune Book",
    "CloudAssignedEntra IDServerData":
"{\"ZeroTouchConfig\":{\"CloudAssignedTenantUpn\":\"\",\"ForcedEnrollment\":1,
\"CloudAssignedTenant
Domain\":\"osddeployment.dk\"}}",
    "CloudAssignedOobeConfig":  1310,
    "CloudAssignedTenantDomain":  "osddeployment.dk",
    "CloudAssignedLanguage":  "os-default"
}
```

Then, you can copy the content of the Autopilot profile to Notepad and save it as `AutopilotConfigurationFile.json`.

Windows devices can be grouped by a correlator `ID` when enrolling using Autopilot for existing devices through Configuration Manager. `ZtdCorrelationId` is a parameter of the Autopilot configuration file. The `enrollmentProfileName` Entra ID device attribute is set to equal `OfflineAutopilotprofile-<correlator ID>` automatically. So, arbitrary Entra ID dynamic groups can be created based on the correlator ID by using the `enrollmentProfileName` attribute.

To create a **Windows Autopilot deployment profile**, perform the following steps:

1. In the Microsoft Intune admin center, choose **Devices** | **Windows** | **Windows enrollment** | **Deployment profiles**.
2. Then, choose **Create profile** | **Windows PC**.
3. In the **Enter a Name for the Profile** field, enter **Autopilot Default profile**.
4. Set **Convert all targeted devices to Autopilot** to **Yes**.

   Select **Yes** to register all targeted devices to Autopilot if they are not already registered, including devices that have gone through the process for Autopilot for existing devices. The next time registered devices go through the Windows OOBE, they will go through the assigned Autopilot scenario.

   Set to **NO** if the profile is a targeted Hybrid Entra joined device, where you plan to have the same devices to be Entra joined in the future. If not, this will mess up your devices in Entra.

5. Leave every other setting as its default unless you have a reason to change them.

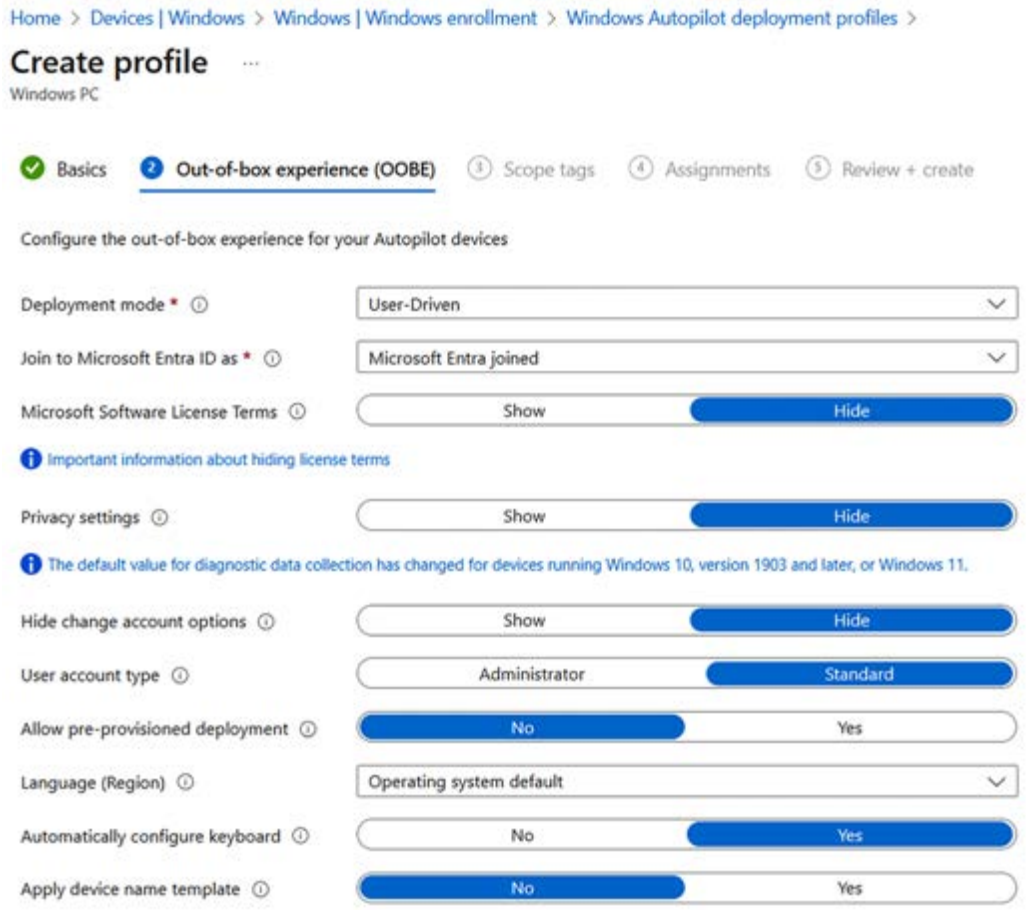


Figure 7.13: Out-of-box experience (OOBE)

In the **Out-of-box experience** (**OOBE**) step, configure the values as you see in *Figure 7.13* and then click **Next.**



Language (Region) requires an Ethernet connection doing the OOBE to have any effect; otherwise, this OOBE wizard will be shown to the end user. The OS default will only have an effect if the OS is a single OS, so this OOBE wizard page will not be shown if the OS is both **en-US** and **nl-NL**, as an example.

Automatically configure keyboard requires an Ethernet connection doing the OOBE to have any effect; otherwise, this OOBE wizard will be shown to the end user.

If an `unattend.xml` file is present on the device during the OOBE phase, Windows Autopilot will most probably fail, so if you are performing the imaging of existing devices, just ensure that files are not present in `%WINDIR%\Panther\Unattend unattend.xml` and `%WINDIR%\Panther\unattend.xml`.

Windows updates during the OOBE

The IT admin cannot opt out of these critical updates as part of the Windows Autopilot provisioning as they are required for the device to operate properly.

Critical driver updates and critical Windows **Zero-Day Patch** (**ZDP**) updates will begin downloading automatically during the OOBE after the user has connected to a network. Thereafter, Autopilot functional and critical updates are automatically downloaded and installed as well.

Feature updates and quality updates will not be updated during this phase of the OOBE.

Windows will alert the user that the device is checking for and applying updates:

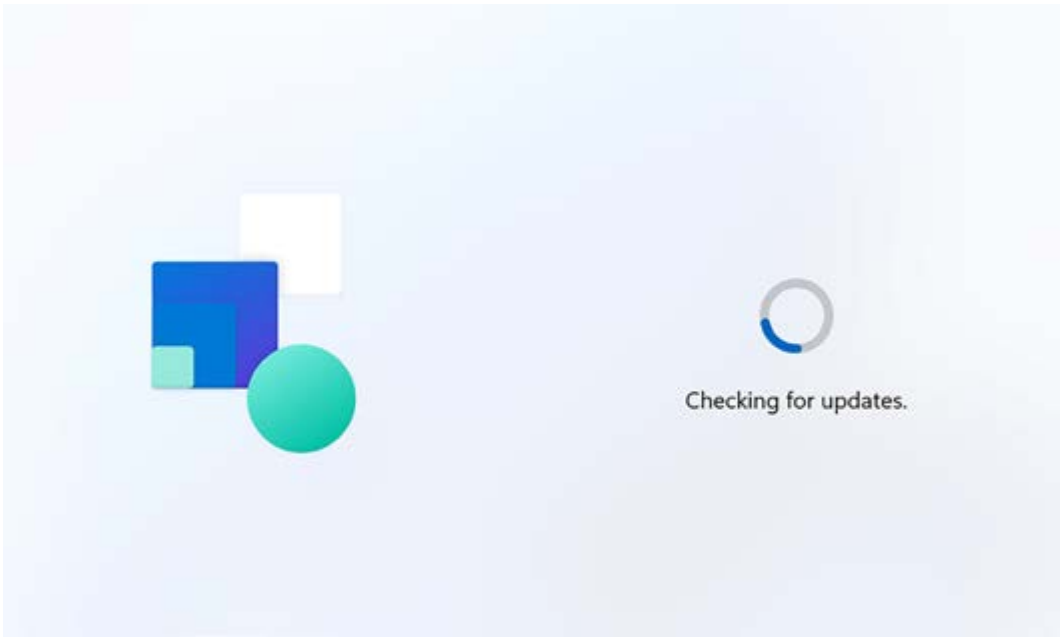


Figure 7.14: Windows checking for updates during the OOBE



If you are using a custom image without any drivers integrated, Windows can download drivers as part of the Windows Autopilot process, and reboots can occur and break the Windows Autopilot experience. The recommendation for Windows Autopilot is to leverage an OEM image for brand-new devices as it includes drivers, as well as a custom image with the correct drivers for existing devices, and also when you are testing Windows Autopilot for existing devices, it gives the best experience and the closest experience to a brand-new device.

Auto-assigning Windows Autopilot profiles in Intune

There are two ways to assign an Autopilot profile to a device from Microsoft Intune – static or dynamic Entra ID groups. Static groups do not give you the automation that you want in an enterprise, so in this section, we will walk you through the automatic profile assignment.

Zero Touch Deployment ID (**ZTDID**) is the unique identifier for a device in the Windows Autopilot service. The ZTDID and group tag are both attributes on the Entra ID device object. The group tag is a value that you can put in the CSV when you are uploading the device to Windows Autopilot, and this value is something that you can choose. You can leverage group tags to group Autopilot devices for a specific purpose, such as an information worker, shared device, Microsoft Teams Rooms system, Kiosk device, or something else. A group tag can be changed in the Autopilot object at a later point in time if you want the device object to be in a different Entra dynamic device group. Remember to click **Sync** in the **Autopilot device** blade; otherwise, you need to wait for the change until the sync has been run in the background every 24 hours.

You will have the standard information – **Device Serial Number**, **Windows Product ID**, and **Hardware Hash** – so you just have to create a custom column named `OrderID` with the value you want to use to create your Autopilot dynamic group for profile assignment – for example, `EdgeKIOSK`.

After importing the Autopilot information into Microsoft Intune, you can use Microsoft Graph Explorer to see the device with the information you just created. You need to look for the Entra ID device object, as the Microsoft Intune device object is only created when Windows executes **Mobile Device Management** (**MDM**) enrollment in Microsoft Intune.

To go to Graph Explorer, visit `https://developer.microsoft.com/en-us/graph/graph-explorer`:

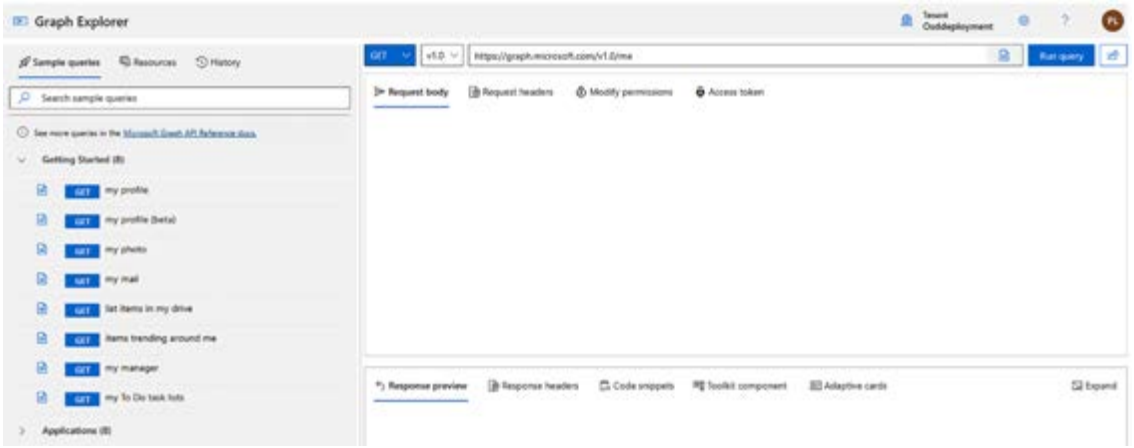


Figure 7.15: Graph Explorer

Signing in to Graph Explorer

Enter `https://graph.microsoft.com/v1.0/devices` to get all the devices – then, you can find the device you just created and see that it has the ZTDID with a unique value, and the group tag is shown as `OrderID` in the graph. You can also run the graph call with the ID at the end and only get the value for a single device: `https://graph.microsoft.com/v1.0/devices/[id]`. The data is stored in a multi-value attribute called `physicalIds`:

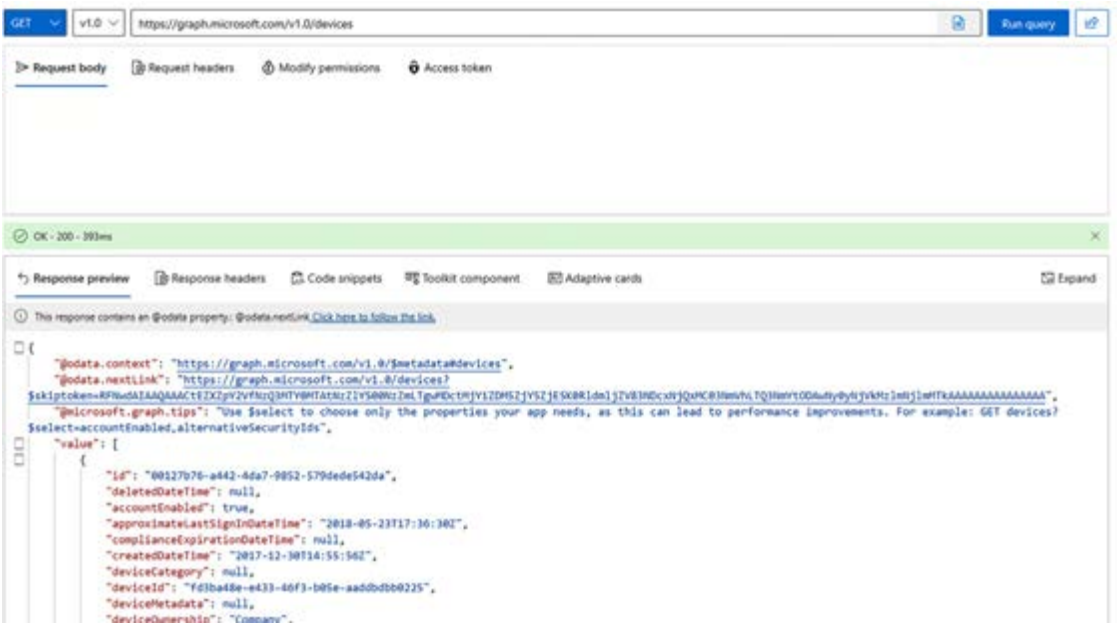


Figure 7.16: Graph Explorer devices

Then, you can find `physicalIds` as an attribute on the device object in the graph output to verify that there is a ZTDID on the Entra ID device object – ZTDID means it is an Autopilot object. You can also see `OrderID` (`OrderID` is the same as a group tag in the Microsoft Intune admin center):

```
"physicalIds": [
    "[HWID]:h:6755414090630361",
    "[ZTDID]:ab1e4d57-66e5-4143-bb43-753be871075f"
    "[OrderId]:EdgeKIOSK",
    "[USER-HWID]:44cd8da3-8f37-49e0-aa01-93c7179969d1:6755414090630361",
    "[GID]:g:6825777827713522",
    "[USER-GID]:44cd8da3-8f37-49e0-aa01-93c7179969d1:6825777827713522",
    ],
```

Now we have all the information we need to create two dynamic Entra ID groups, one for all Autopilot devices and one for `EdgeKIOSK`.

We will create three dynamic groups so we can distinguish between the different Windows Autopilot scenarios. We are naming the groups `All AutoPilot Devices`, `All AutoPilot EdgeKIOSK`, and `All AutoPilot JSON`:

In the Microsoft Intune admin center (`https://intune.microsoft.com/`), choose **Groups**:

1. Choose **New Group**.
2. Enter `All Autopilot Devices` in the **Group name** field.

3. Choose **Dynamic Device** for **Membership type:**

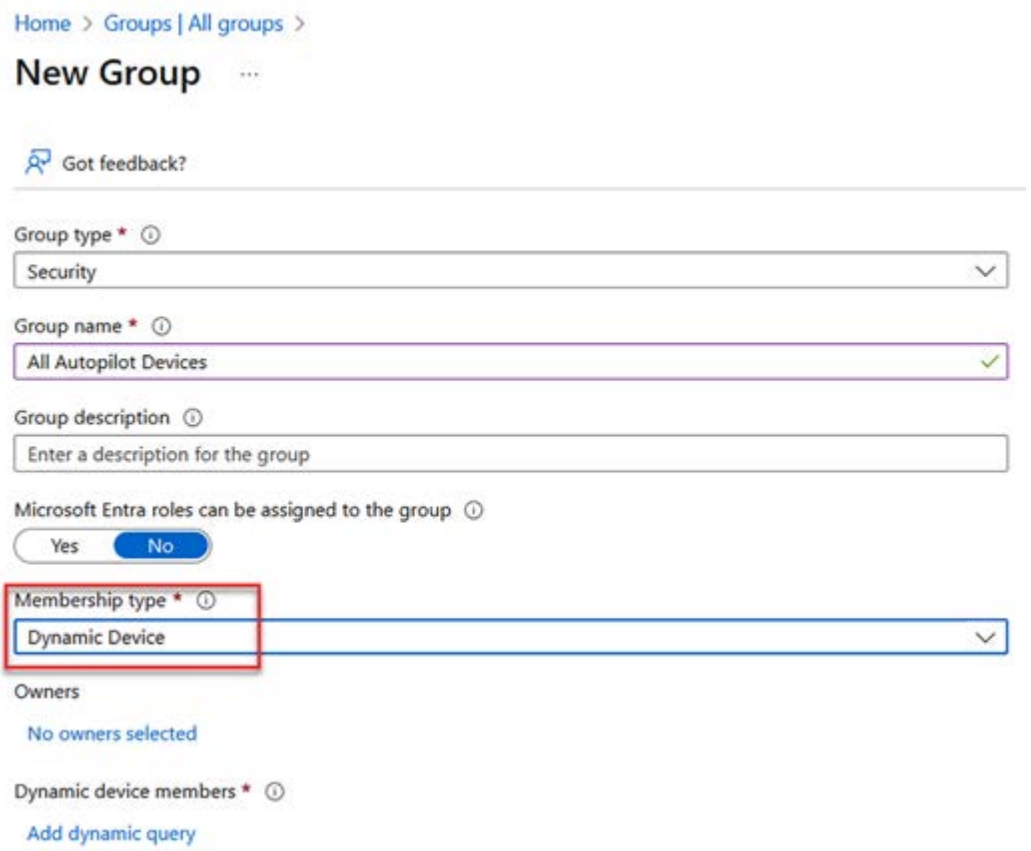


Figure 7.17: New Entra ID device group

The first group, **All AutoPilot Devices**, has a dynamic group membership rule such as this:

```
(device.devicePhysicalIDs -any (_ -startsWith "[ZTDid]")) -and -not (device.
devicePhysicalIDs -any _ -eq "[OrderID]: EdgeKIOSK")
```

This rule will find all devices with the ZTDID and exclude all devices where the value of **OrderID** is **EdgeKIOSK**:



Figure 7.18: Entra ID group Autopilot rule syntax

The second group, **All AutoPilot EdgeKIOSK**, has a dynamic group membership rule such as this: `(device.devicePhysicalIds -any _ -eq "[OrderID]: EdgeKIOSK")`.

This rule will find all devices where the value of **OrderID** is equal to **EdgeKIOSK**.

You can also just create the Entra ID dynamic groups with PowerShell:

```
Install-Module -Name Microsoft.Graph
Connect-MgGraph -Scopes "Group.ReadWrite.All"

 #All AutoPilot Devices

$AllAutopilotDevices = @{

    DisplayName = "All AutoPilot Devices"

    Description = "All AutoPilot Devices"

    mailNickname = "AllAutopilotDevices"
```

```
    MailEnabled = $false
    SecurityEnabled = $true
    GroupTypes = @(
        "DynamicMembership"
    )
    MembershipRule = 'device.devicePhysicalIDs -any _ -startsWith "[ZTDid]"'
    MembershipRuleProcessingState = "On"
}
New-MgGroup -BodyParameter $AllAutopilotDevices


#All AutoPilot EdgeKIOSK
$AllAutopilotEdgeKIOSK = @{
    DisplayName = "All AutoPilot EdgeKIOSK"
    Description = "All AutoPilot EdgeKIOSK"
    mailNickname = "AllAutopilotEdgeKIOSK"
    MailEnabled = $false
    SecurityEnabled = $true
    GroupTypes = @(
        "DynamicMembership"
    )
    MembershipRule = 'device.devicePhysicalIds -any _ -eq
```

```
"[OrderID]:EdgeKIOSK"'

    MembershipRuleProcessingState = "On"

}

New-MgGroup -BodyParameter $AllAutopilotEdgeKIOSK



#All AutoPilot JSON

$AllAutopilotJSON = @{

    DisplayName = "All AutoPilot JSON"

    Description = "All AutoPilot JSON"

    mailNickname = "AllAutopilotJSON"

    MailEnabled = $false

    SecurityEnabled = $true

    GroupTypes = @(

        "DynamicMembership"

    )

    MembershipRule = 'device.enrollmentProfileName -eq
"OfflineAutopilotprofile-264c05b0-683c-4537-87ff-1ff5151d5b98"'

    MembershipRuleProcessingState = "On"

}

New-MgGroup -BodyParameter $AllAutopilotJSON
```

Now, you have imported the hardware information into Windows Autopilot and created all the groups you need to process by configuring the enrollment status page.

Enrollment Status Page (ESP)

Many think that the ESP and Windows Autopilot are one and the same. That is not necessarily the whole truth as the ESP is a core Windows function and can be set as a Windows **Configuration Service Provider** (**CSP**). CSPs are explained in depth in *Chapter 9*.

The ESP can be used as part of any Windows Autopilot provisioning scenario. It can also be used separately from Windows Autopilot as part of the default OOBE for Entra ID join, as well as for any new users signing in to the device for the first time.

Basically, what that means is that any Windows 10/Windows 11 devices that join Entra ID in the OOBE phase will have the ESP shown to the end user, irrespective of whether it is a Windows Autopilot device, as long as there is an ESP assigned to the user or device.

You can create multiple ESP profiles with different configurations that specify the following:

- Showing the installation progress
- Blocking access until the provisioning process is complete
- Time limits
- Allowed troubleshooting operations

We will show you how to do this in this section and, in a later section, with a Windows Autopilot Kiosk scenario.

ESP implementation – Windows CSP

The ESP uses the `EnrollmentStatusTracking` CSP and the `FirstSyncStatus` CSP to track the installation of different apps:

- The `EnrollmentStatusTracking` CSP: `/Vendor/MSFT/EnrollmentStatusTracking`.
- The `EnrollmentStatusTracking` CSP: **Windows Client Management | Microsoft Docs** (`https://docs.microsoft.com/en-us/windows/client-management/mdm/enrollmentstatustracking-csp`).

- The `EnrollmentStatusTracking` CSP is supported in Windows 10 version 1903 and later.
- The `EnrollmentStatusTracking` CSP is used to track the installation of the Microsoft Intune management extension and Microsoft Intune Win32 apps that are the target devices and/or users that are blocked by the ESP.
- The `FirstSyncStatus` CSP: `./Vendor/MSFT/DMClient/Provider/ProviderID/FirstSyncStatus`.
- The DMClient CSP – Windows Client Management | Microsoft Docs (`https://docs.microsoft.com/en-us/windows/client-management/mdm/dmclient-csp`).
- The `FirstSyncStatus` CSP is supported in Windows 10 version 1709 and later.
- The `FirstSyncStatus` CSP is responsible for delivering the ESP CSP payload from Microsoft Intune to the Windows client. The payload includes ESP settings such as the timeout period and applications that are required to be installed. It also delivers the expected **Microsoft Installer** (**MSI**) (line-of-business) applications, Microsoft Store for Business apps, Wi-Fi profiles, and **Simple Certificate Enrollment Protocol** (**SCEP**) certificate profiles, as well as policies for Microsoft Edge, assigned access, and Kiosk Browser.

We will look at the steps to create an ESP, as follows:

1. Create the first ESP by starting up the Microsoft Intune admin center (`https://intune.microsoft.com/`), and choose **Devices** | **Windows** | **Windows enrollment** | **Enrollment Status Page**.
2. Choose a profile under **Settings**.
3. Choose **Yes** for **Show app and profile installation progress**.
4. Choose **Yes** for **Block device use until all apps and profiles are installed**.

5. In the **Settings** step, configure the following values and then click **Next:**

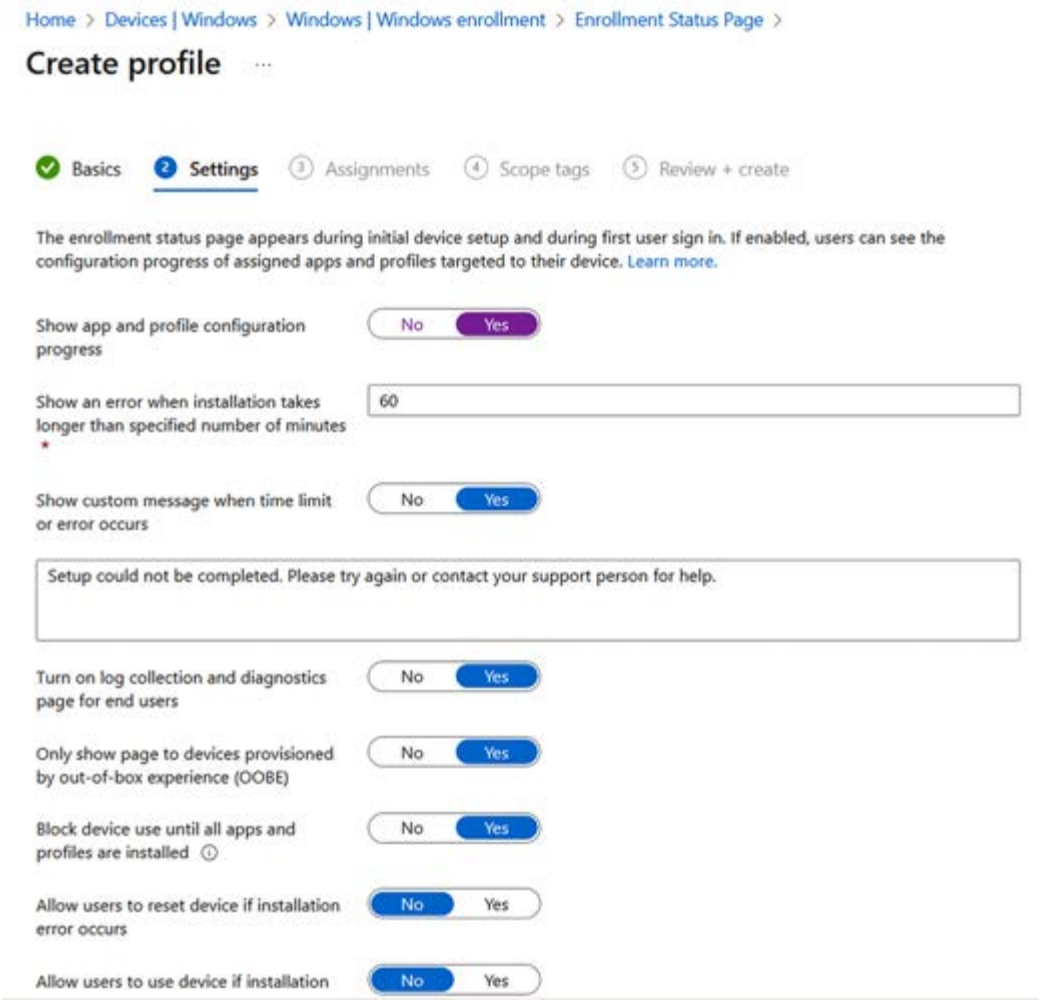


Figure 7.19: Enrollment Status Page

6. Choose **Selected** for **Block device use until required apps are installed if they are assigned to the user/device.**

7. Click **Select apps**, and then click **Select** | **Save** for the apps.

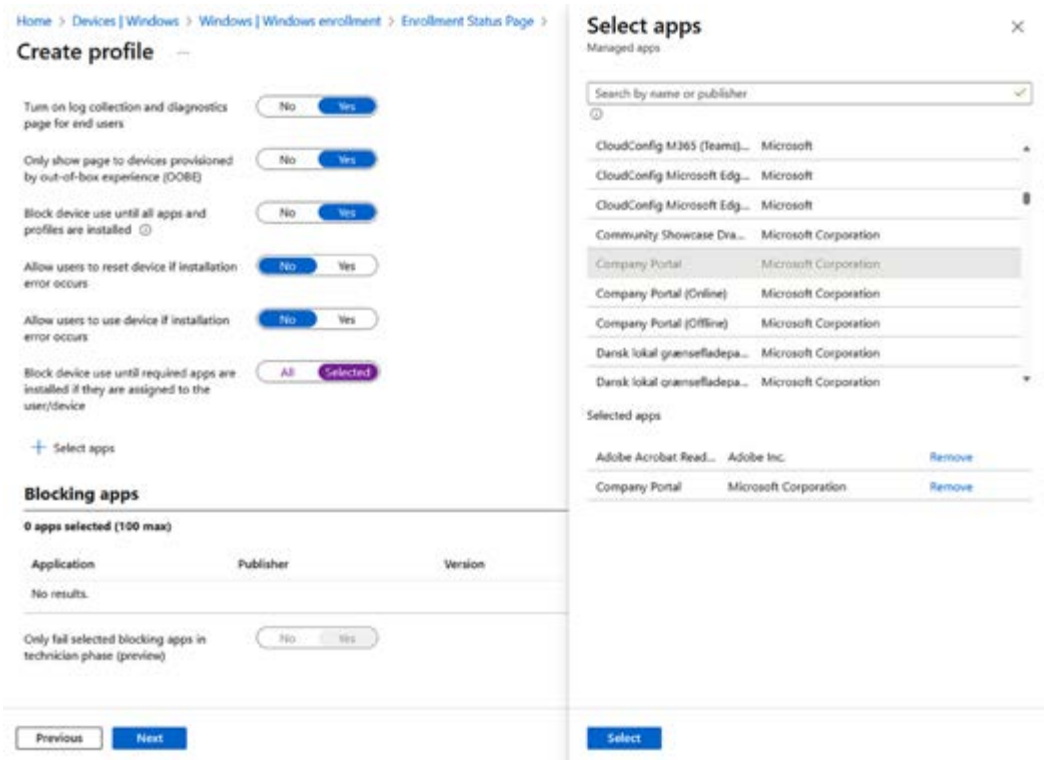


Figure 7.20: Enrollment Status Page configuration

Only block apps that you need for security reasons and/or apps that are needed on the device for the end user to have the best experience with their brand-new device.

Now that we have seen how to create an enrollment page, let's move on and learn about Autopilot reporting and diagnostics.

Autopilot reporting and diagnostics

Ensure that **Device diagnostics** is enabled for Autopilot scenarios in your tenant. This will automatically capture diagnostic logs if the Autopilot process fails and upload the logs to your Intune tenant, where you can access them on the device in Intune:

1. Start the Microsoft Intune admin center (`https://intune.microsoft.com/`), and choose **Tenant administration** | **Device diagnostics**.

2. Ensure that the toggle is set to **Enabled:**



Figure 7.21: Enabling Device diagnostics

On a Windows Autopilot device, run `cmd.exe` as an administrator, and then you can run `MdmDiagnosticsTool` to get the Windows Autopilot diagnostic logs directly from the local device:

```
c:\windows\system32\MdmDiagnosticsTool.exe -area Autopilot -cab C:\temp\
MdmDiagnostics.cab
```

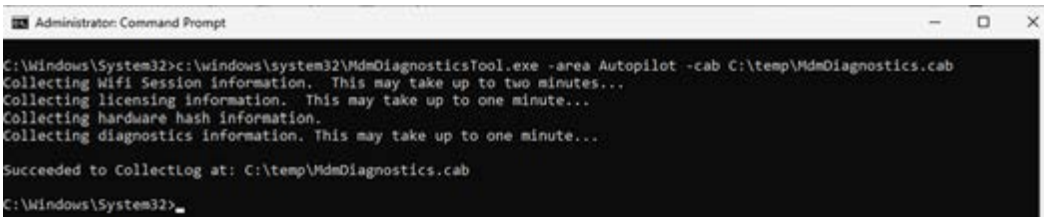


Figure 7.22: MdmDiagnosticsTool

You will then get the `MdmDiagnostics.cab` file, where you can extract the content to a folder to get access to the content:

```
A2757648-0D43-4494-B139-FAE71012F565_Device_00787de3-c700-0df8-b2bc-66d3de6913
26_49ffce6e4a8bba20c8a50dfee53ba60700d59d910ea41f62345480cfcd43f026_29BDDEA2-
8227-4495-86F6-3384E5B5AD65.xml
A2757648-0D43-4494-B139-FAE71012F565_Device_393ad4b3-0107-5ef3-df0c-90f271abb3
77_480c0c8260ee4d7864ea3cc0b393faec41ac9fe2b25ca51120f7badc46d0a9ef_FEEC5786-
D652-4526-A6B3-BBDCDD1E05DF.xml
AgentExecutor.log
AppActionProcessor.log
AutopilotDDSZTDFile.json
ClientHealth.log
CloudExperienceHostOobe.etl.001
CloudExperienceHostOobe.etl.002
CloudExperienceHostOobe.etl.003
DeviceHash_WIN11-23H2.csv
```

```
DeviceHealthMonitoring.log
DiagnosticLogCSP_Collector_Autopilot_2023_12_10_17_53_25.etl
DiagnosticLogCSP_Collector_Autopilot_2023_12_6_3_46_32.etl
DiagnosticLogCSP_Collector_Autopilot_2023_12_6_4_27_21.etl
DiagnosticLogCSP_Collector_Autopilot_2023_12_6_4_28_55.etl
DiagnosticLogCSP_Collector_DeviceProvisioning_2023_12_10_13_52_41.etl
DiagnosticLogCSP_Collector_DeviceProvisioning_2023_12_6_18_17_45.etl
DiagnosticsFrameworkData.json
HealthScripts.log
IntuneManagementExtension.log
LicensingDiag.cab
LicensingDiag_Output.txt
list.txt
MdmDiagLogMetadata.json
MdmDiagReport_RegistryDump.reg
MdmLogCollectorFootPrint.txt
microsoft-windows-appxdeploymentserver-operational.evtx
microsoft-windows-assignedaccess-admin.evtx
microsoft-windows-assignedaccessbroker-admin.evtx
microsoft-windows-assignedaccessbroker-operational.evtx
microsoft-windows-assignedaccess-operational.evtx
microsoft-windows-crypto-ncrypt-operational.evtx
microsoft-windows-devicemanagement-enterprise-diagnostics-provider-admin.evtx
microsoft-windows-devicemanagement-enterprise-diagnostics-provider-autopilot.
evtx
microsoft-windows-devicemanagement-enterprise-diagnostics-provider-debug.evtx
microsoft-windows-devicemanagement-enterprise-diagnostics-provider-operational.
evtx
microsoft-windows-laps-operational.evtx
microsoft-windows-moderndeployment-diagnostics-provider-autopilot.evtx
microsoft-windows-moderndeployment-diagnostics-provider-diagnostics.evtx
microsoft-windows-moderndeployment-diagnostics-provider-managementservice.evtx
microsoft-windows-provisioning-diagnostics-provider-admin.evtx
microsoft-windows-shell-core-operational.evtx
microsoft-windows-user device registration-admin.evtx
microsoft-windows-aad-operational.evtx
Sensor.log
setupact.log
TpmHliInfo_Output.txt
UEFI_Data_Output.txt
Wifi.etl
Win32AppInventory.log
```

The most important information you will get from the MDM diagnostics tools is as follows:

```
Registry Dump
MdmDiagReport_RegistryDump.reg captures the
HKEY_LOCAL_MACHINE
HKEY_ CURRENT_USER
Registry values associated with autopilot device provisioning are written to
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Provisioning\Diagnostics\AutoPilot
HKEY_CURRENT_USER\software\microsoft\enterprisemodernappmanagement and HKEY_
LOCAL_MACHINE\software\microsoft\enterprisemodernappmanagement
In the Microsoft Intune admin center, there is a Windows Autopilot deployment
report. To access it, use the following process:
```

In the Microsoft Intune admin center (`https://intune.microsoft.com/`), choose **Devices** | **Monitor** | **Autopilot deployments (preview)**.

You can see your Windows Autopilot deployments from the last 30 days:



Figure 7.23: Autopilot report

You can see the following attributes:

- **Enrollment date**
- **Enrollment method**
- **Serial number**
- **Device name**
- **User**
- **Autopilot profile**
- **Enrollment status page deployment state**
- **Deployment total time**

Company Portal

The Company Portal is a self-service tool for end users, in which the end user can install apps that the IT admin has made available to them, check for device compliance, and so on. They can also do other actions such as syncing the device, reviewing the download status, or checking the compliance of the users' devices.

For Windows Autopilot-provisioned devices, it is recommended that you install the Company Portal in the system context. The Company Portal app will be installed in the device context when assigned to the Autopilot device group and will be installed on the device before the first user logs in. You can choose to install the Company Portal app using the steps shown next:

1. In the Microsoft Intune admin center (`https://intune.microsoft.com/`), choose **Apps** | **Windows**.
2. Click **Add**.
3. Select **App type** | **Microsoft Store app (new)**.
4. Click **Select**.
5. Click **Search the Microsoft Store app (new)**.
6. Search for `company portal`:



Figure 7.24: Microsoft Store app (new)

7. Select **System:**

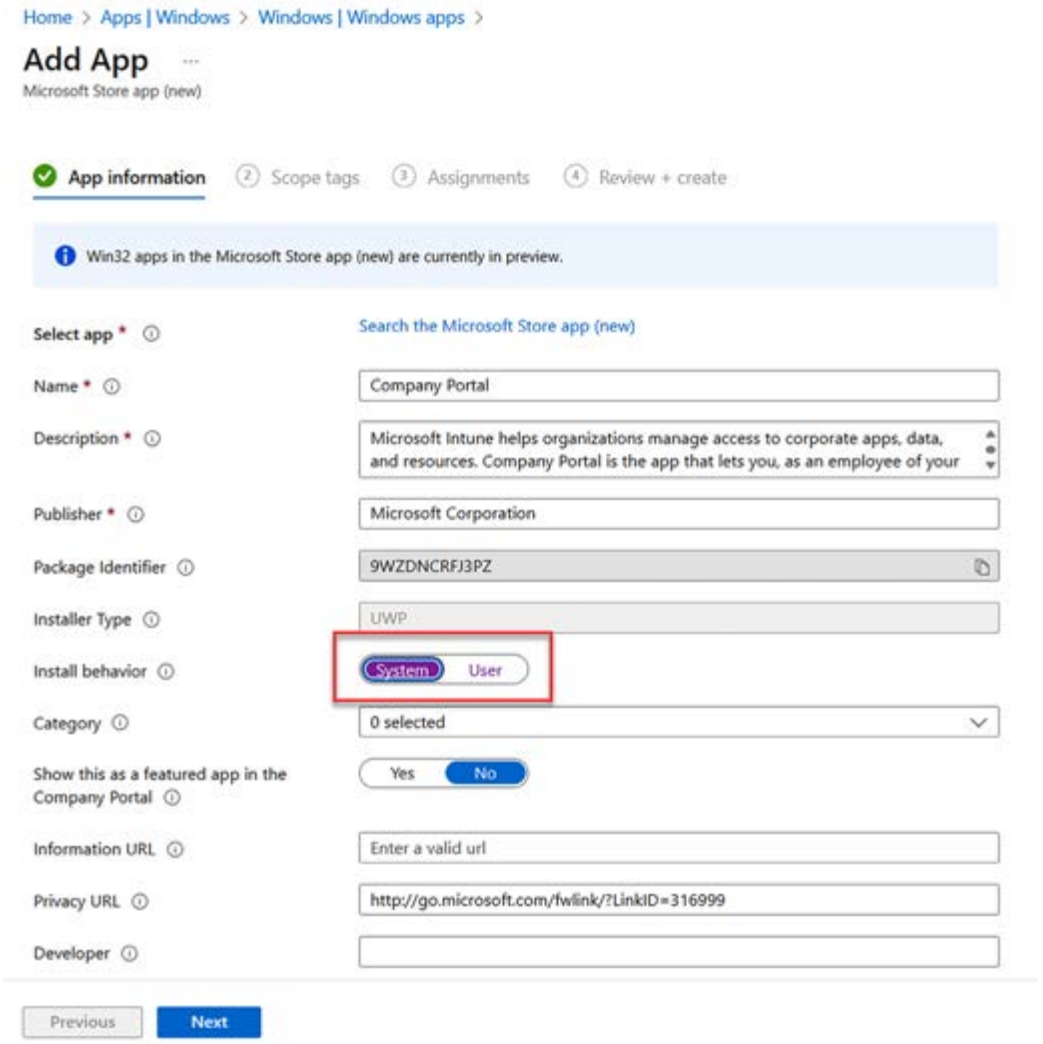


Figure 7.25: Add App

8. Assign the Company Portal app as a required app to your selected Autopilot device group.

Configuring automatic BitLocker encryption for Autopilot devices

With Windows Autopilot, BitLocker encryption settings can be configured to be applied before automatic encryption starts. Any Windows devices that do Entra join from OOBE will be automatically BitLocker-encrypted with the default values. This configuration ensures that the default encryption algorithm is not applied automatically. Other BitLocker policies can also be applied before automatic BitLocker encryption begins.

BitLocker automatic device encryption uses BitLocker drive encryption technology to automatically encrypt internal drives after the user completes the OOBE on *Modern Standby* or **Hardware Security Testability Specification** (**HSTI**)*-compliant hardware*.

In the case of Modern Standby requirements or HSTI validation, this requirement is met by one of the following:

- The Platform Secure Boot self-test (or additional self-tests as configured in the registry) must be reported by the HSTI as implemented and passed.
- Excluding Thunderbolt, the HSTI must not report any non-allowed DMA buses.
- If Thunderbolt is present, the HSTI must report that Thunderbolt is configured securely (the security level must be SL1 – *User Authorization* or higher).

Modern Standby requirements are implemented. These include requirements for **Unified Extensible Firmware Interface** (**UEFI**) Secure Boot and protection from unauthorized **Direct Memory Access** (**DMA**).

Starting with *Windows 10 version 1703*, this requirement can be met through an HSTI test.

Windows (Modern Standby) expands the *Windows 8.1 Connected Standby power model*. Connected Standby (and consequently, Modern Standby) enables an instant on/instant off user experience, like smartphone power models. Just like a phone, the S0 low-power idle model enables the system to stay connected to the network while in a low-power mode.

By leveraging the `powercfg/a` command, you can see whether your device supports Modern Standby (**S0 Low Power Idle**):

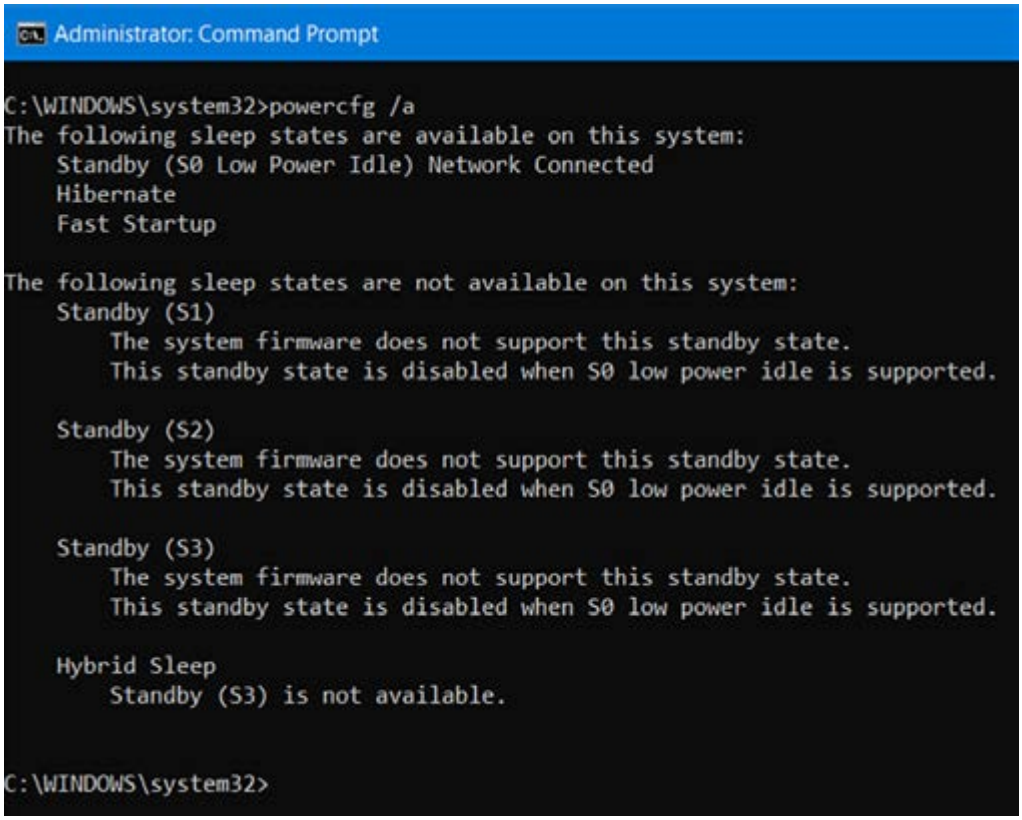


Figure 7.26: powercfg Modern Standby



BitLocker automatic device encryption starts during the OOBE experience. However, BitLocker drive protection is enabled only after users sign in with an Entra ID account. Until then, protection is suspended, and data is not protected.

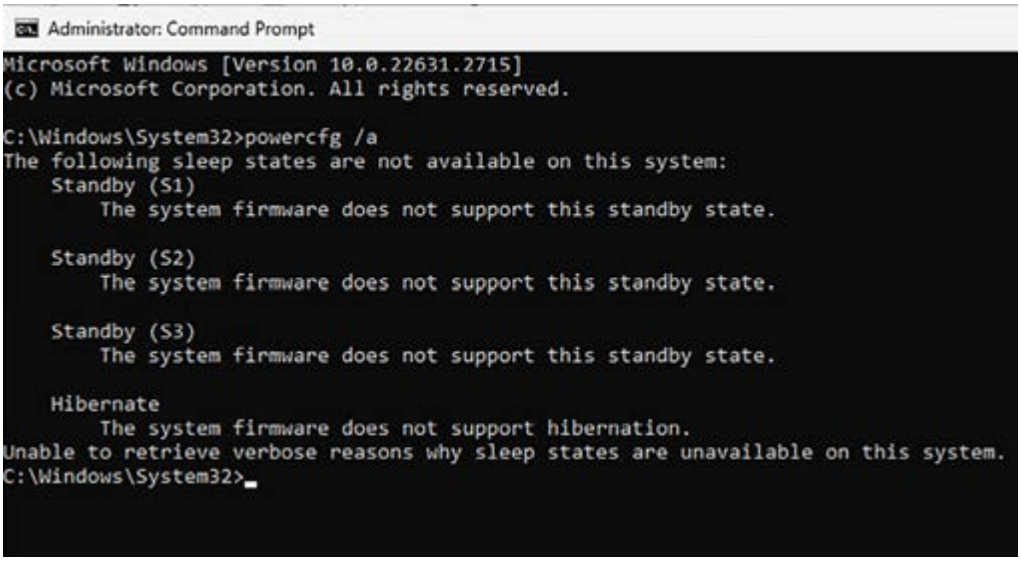


Figure 7.27: powercfg Non-Modern Standby

The BitLocker encryption algorithm is used when BitLocker is first enabled. The algorithm sets the strength for full-volume encryption. Available encryption algorithms are `AES-CBC 128-bit`, `AES-CBC 256-bit`, `XTS-AES 128-bit`, and `XTS-AES 256-bit` encryption. BitLocker will use the default encryption method of `XTS-AES 128-bit` or the encryption method specified by any setup script.

To make sure the BitLocker encryption algorithm you want is set before automatic encryption occurs for Autopilot devices, make sure the following requirements are fulfilled:

- The device contains a **Trusted Platform Module** (**TPM**), either TPM 1.2 or TPM 2.0.
- UEFI Secure Boot is enabled.
- Platform Secure Boot is enabled.
- DMA protection is enabled.
- Configure the **Encryption method** settings in the BitLocker policy to the encryption algorithm you want.
- Assign the policy to your Autopilot device group. The encryption policy must be assigned to devices in the group, not users.
- Enable the Autopilot ESP for these devices. If the ESP is not enabled, the policy won't apply before encryption starts.



When you enable **EncryptionMethodByDriveType**, you must specify values for all three drives (OS, fixed data, and removable data); otherwise, it will fail (**500** return status). For example, if you only set the encryption method for the OS and removable drives, you will get a **500** return status in the policy status.

Create the BitLocker policy in Intune for automatic BitLocker encryption as follows:

1. In the Microsoft Intune admin center (`https://intune.microsoft.com/`), choose **Endpoint Security** | **Disk Encryption**.
2. Choose **Create policy**.
3. Select **Platform** | **Windows 10 and later**.
4. Select **Profile type** | **BitLocker**.
5. Select **Name** | **Autopilot BitLocker** | **Next**.
6. Expand **BitLocker**.
7. Select **Require Device Encryption:**

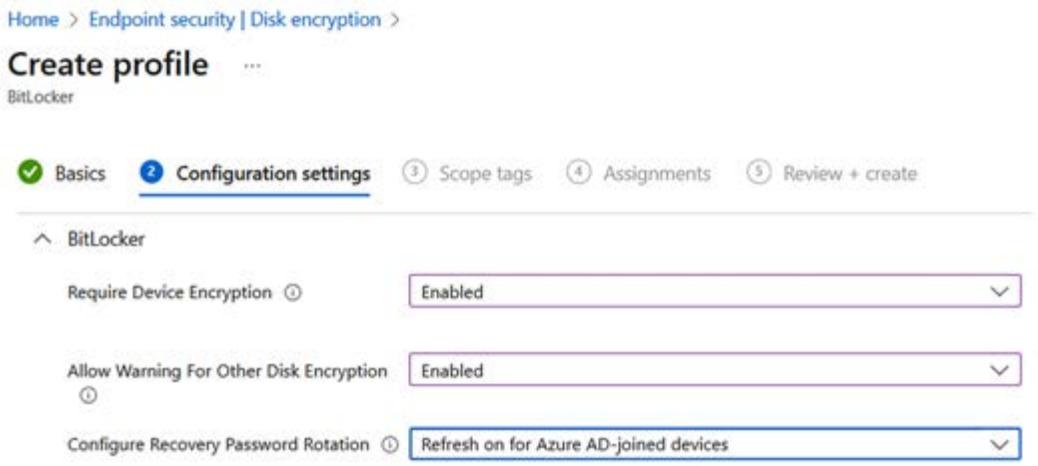


Figure 7.28: Windows encryption

The BitLocker base settings should be as follows:

1. Set **Allow Warning For Other Disk Encryption** to **Enabled**.

   Selecting **Enabled** will disable the BitLocker configuration prompt and the warning prompt for other disk encryptions. Block is needed here to BitLocker-encrypt a device automatically, including the possibility for Windows to prompt for a BitLocker PIN.

2. Set **Configure Recovery Password Rotation** to **Refresh on for Azure AD-joined devices**. This allows the admin to configure numeric recovery password rotation upon use for OS and fixed drives on Entra ID and hybrid domain-joined devices. When not configured, rotation is turned on by default for Entra ID only, and off for hybrid. The policy will be effective only when Active Directory backup for recovery password is configured to be required. For OS drives, turn on **Do not enable BitLocker until recovery information is stored to AD DS for operating system drives**. For fixed drives, turn on **Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives**. Supported values are 0 (Numeric Recovery Password Rotation OFF), 1 (Numeric Recovery Password Rotation upon use ON for AAD-joined devices), and the default value of 2 (Numeric Recovery Password Rotation upon use ON for both AAD and hybrid devices). If you want to disable this policy, use the following SyncML: `112./Device/Vendor/MSFT/BitLocker/ConfigureRecoveryPasswordRotationint0`.
3. Expand **Administrative Templates**.
4. For **Configure encryption methods**, select what your organization requires. The Windows default is `XTS-AES 128-bit`, which is also the recommended value in the Windows security baseline:

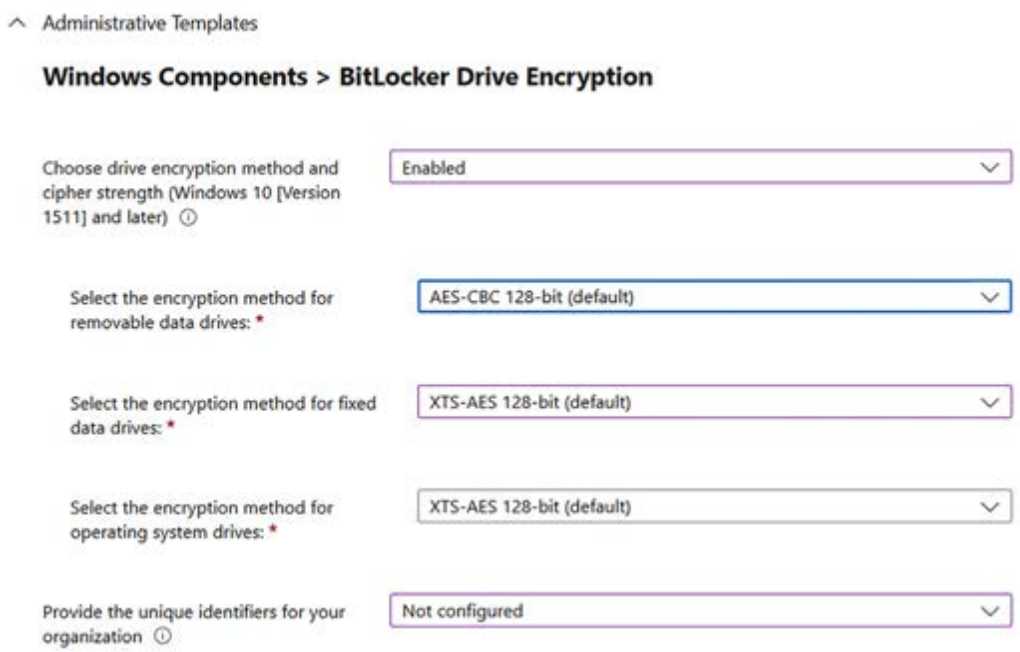


Figure 7.29: BitLocker base settings

5. Some other security baselines recommend 256-bit encryption methods. An example is **CIS Microsoft Intune for Windows 11**, which can be configured within the BitLocker policy:

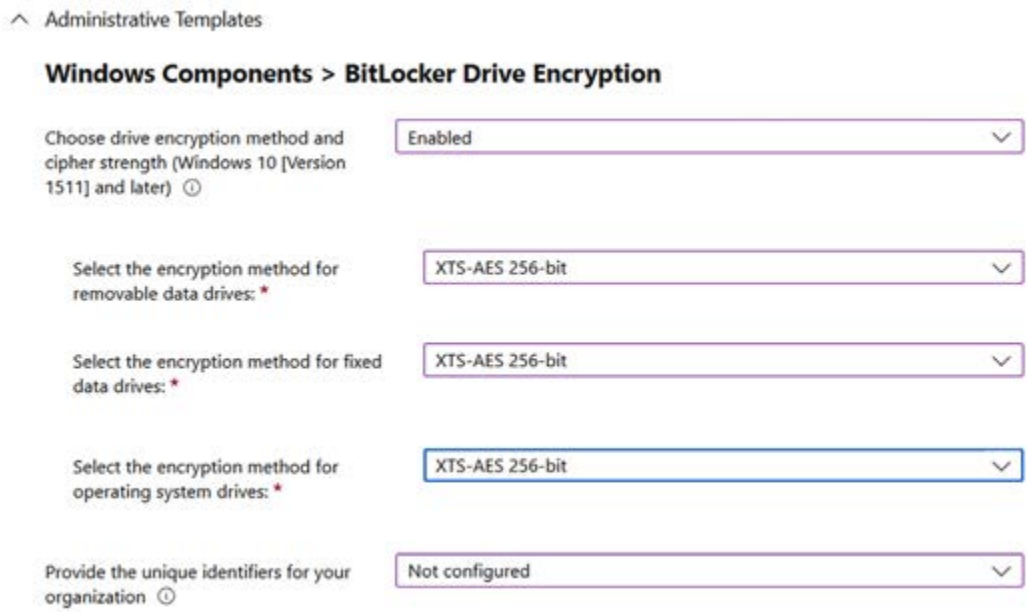


Figure 7.30: BitLocker 256-bit encryption method



Be aware of how you are assigning this policy as the policy settings need to be applied to the device before encryption is started on the device.

Therefore, always assign your BitLocker policy to your Entra ID device group that contains your Autopilot devices.

This policy setting allows you to configure the encryption type used by BitLocker Drive Encryption. This policy setting is applied when you turn on BitLocker. Changing the encryption type has no effect if the drive is already encrypted or if encryption is in progress. Choose **Full encryption** to require that the entire drive is encrypted when BitLocker is turned on. Choose **Used Space Only encryption** to require that only the portion of the drive used to store data is encrypted when BitLocker is turned on. If you enable this policy setting, the encryption type that BitLocker will use to encrypt drives is defined by this policy and the encryption type option will not be presented in the BitLocker setup wizard. If you disable or do not configure this policy setting, the BitLocker setup wizard will ask the user to select the encryption type before turning on BitLocker.

The BitLocker OS drive settings are as follows:

1. Set **Enforce drive encryption type on operating system drives** to **Enabled:**
2. For **Select the encryption type: (Device)**, select **Used Space Only encryption:**

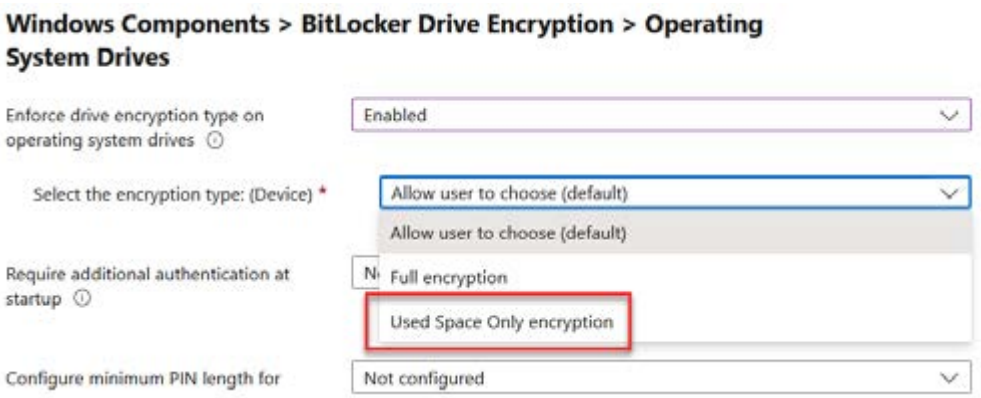


Figure 7.31: BitLocker OS drive settings

3. Set **Choose how BitLocker-protected operating system drives can be recovered** to **Enabled.**
4. Set **Store recovery information in Azure Active Directory before enabling BitLocker** to **True.** This will prevent users from enabling BitLocker unless the computer successfully backs up the BitLocker recovery information to **Entra ID.** Selecting **Require** will ensure that the recovery keys are successfully stored in Entra ID before enabling encryption.
5. Set **Save BitLocker recovery information to Azure Active Directory** to **True.**
6. Enable the **BitLocker recovery information** to be stored in Entra ID on the device object, so end users can retrieve it themselves on devices where they are the primary users. The Entra ID admin with the right privileges can always retrieve the BitLocker recovery key.

This policy setting allows you to control how BitLocker-protected OS drives are recovered in the absence of the required startup key information.

This policy setting is applied when you turn on BitLocker. The **Allow certificate-based data recovery agent** checkbox is used to specify whether a data recovery agent can be used with BitLocker-protected OS drives.

Before a data recovery agent can be used, it must be added from the **Public Key Policies** item in either the Group Policy Management Console or Local Group Policy Editor. Consult the **BitLocker Drive Encryption Deployment Guide** on Microsoft TechNet for more information about adding data recovery agents.

In **Configure user storage of BitLocker recovery information**, select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

Select **Omit recovery options from the BitLocker setup wizard** to prevent users from specifying recovery options when they turn on BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you turn on BitLocker; instead, BitLocker recovery options for the drive are determined by the policy setting.

In **Save BitLocker recovery information to Active Directory Domain Services**, choose which BitLocker recovery information to store in AD DS for OS drives. If you select **Backup recovery password and key package**, both the BitLocker recovery password and key package are stored in AD DS.

Storing the key package supports recovering data from a drive that has been physically corrupted. If you select **Backup recovery password only**, only the recovery password is stored in AD DS.

Select the **Do not enable BitLocker until recovery information is stored in AD DS for operating system drives** checkbox if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.



If the **Do not enable BitLocker until recovery information is stored to AD DS for operating system drives** option is set to **True**, a recovery password is automatically generated.

If you enable this policy setting, you can control the methods available to users to recover data from BitLocker-protected OS drives. If this policy setting is disabled or not configured, the default recovery options are supported for BitLocker recovery.

By default, a **Data Recovery Agent** (**DRA**) is allowed, the recovery options can be specified by the user (including the recovery password and recovery key), and recovery information is not backed up to AD DS.

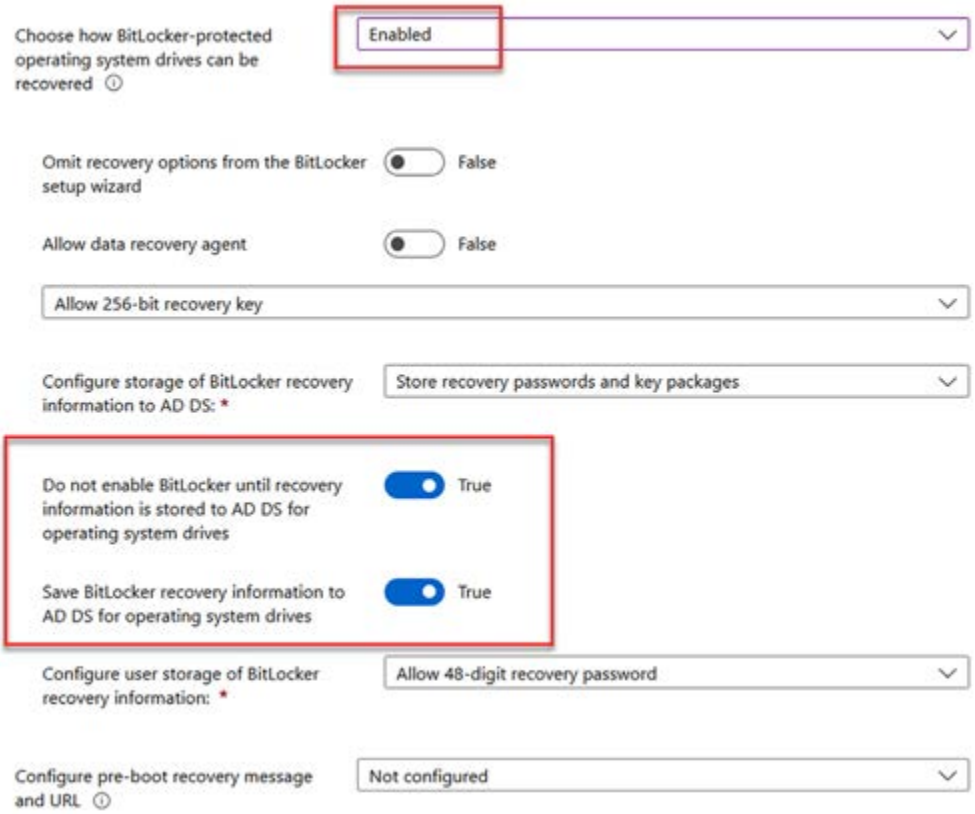


Figure 7.32: BitLocker storage recovery information



If testing Autopilot and BitLocker encryption on Hyper-V or any other virtual platform, we recommend you have 4 GB of memory assigned and 2–4 virtual CPUs (4 is better for performance).

For automatic BitLocker encryption to work, you need to enable **Trusted Platform Module** on the virtual device:

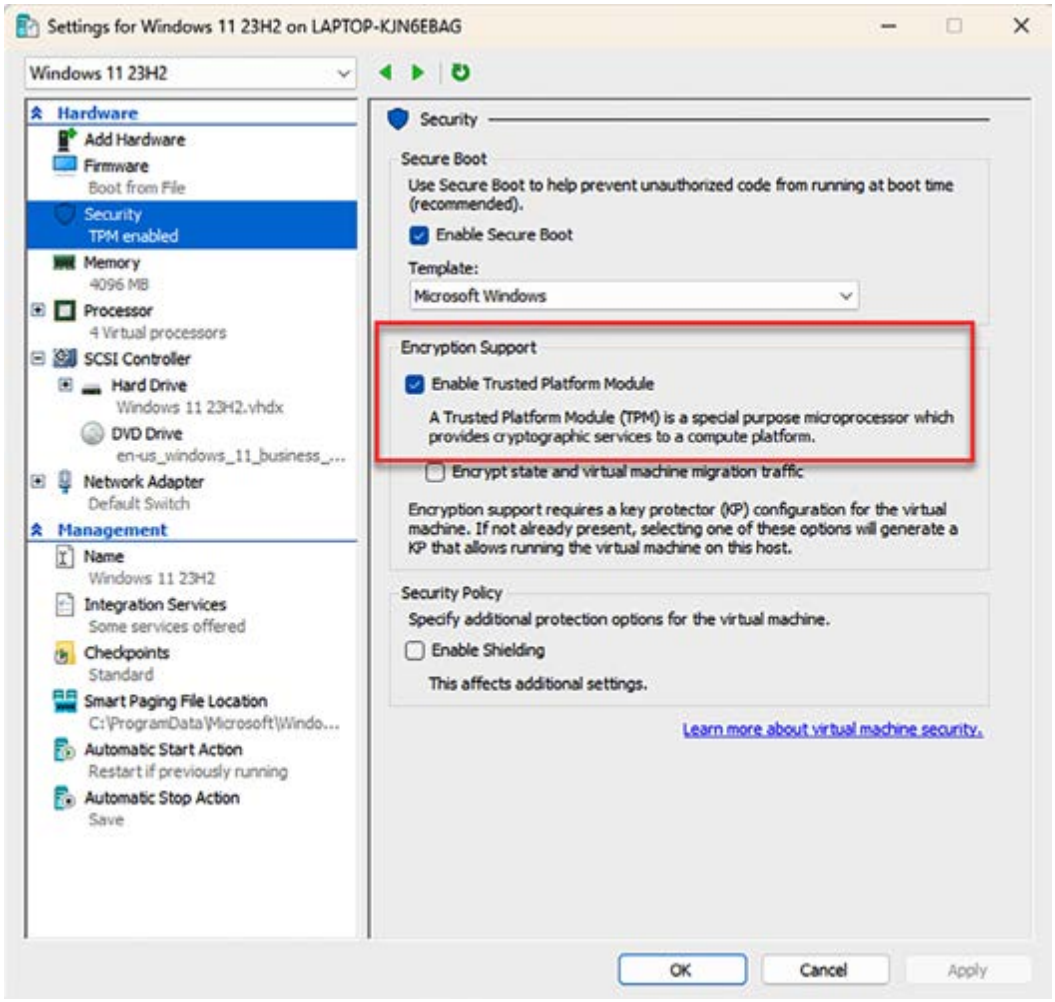


Figure 7.33: Hyper-V encryption support

When testing on a virtual machine hosted on Hyper-V, you might experience different behavior than if you are testing on a physical device. Some IT admins tend to use snapshots; when a virtual device is reverted to a previous snapshot, MDM synchronization on the devices may not work at first.

To start easily testing Autopilot, there is already a guided scenario called cloud configuration in Microsoft Intune. This will be covered in the next section.

Troubleshooting automatic BitLocker encryption on a VM

The two most common reasons why BitLocker automatic encryption does not kick in are:

- The BitLocker policy is not configured correctly.
- BitLocker drive encryption cannot start if there is a removal drive in the device.

When you install a test device in your local Hyper-V environment, you need to do it from an ISO. That ISO is mounted on the device and, therefore, is seen as bootable media:

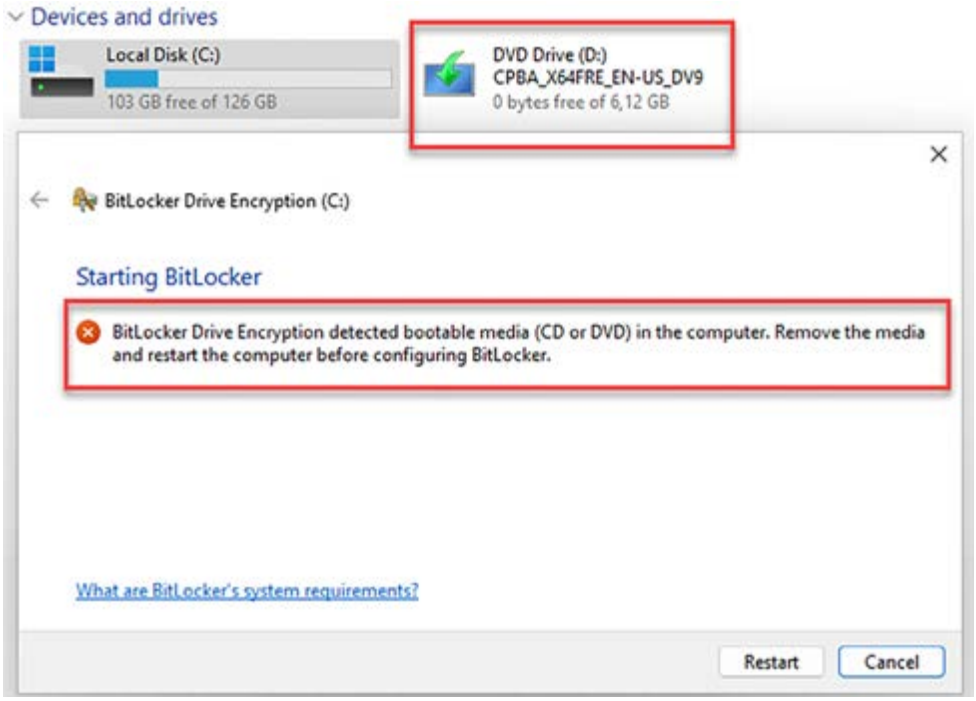


Figure 7.34: Bootable media detected

As you can see in the screenshot above, this has nothing to do with Microsoft Intune, but with how Windows functions. There is a quick fix: just unmount the ISO in Hyper-V and then do an MDM sync or reboot the device and BitLocker encryption will start.

Windows Hello for Business

Windows Hello for Business is a solution that replaces passwords with strong two-factor authentication on devices. It uses biometrics or a PIN to authenticate users to Microsoft Entra, Active Directory, and other identity providers. It is available for Windows 10 and later versions.

Windows Hello for Business is a distributed system that uses several components to accomplish device registration, provisioning, and authentication. The following are the categories of components that support Windows Hello for Business:

- **Identity Provider (IdP)**: The IdP is responsible for verifying the user's identity and issuing a certificate to the user's device.
- **Registration Authority (RA)**: The RA is responsible for verifying the user's identity and issuing a certificate to the user's device.
- **Key Trustee (KT)**: The KT is responsible for managing the keys used to encrypt and decrypt the user's data.
- **Device**: The device is responsible for storing the user's certificate and private key.

Windows Hello for Business provides several benefits over traditional password-based authentication:

- **Stronger security**: Biometric authentication is more secure than passwords because it is harder to crack.
- **Improved user experience**: Users can sign in to their devices and applications quickly and easily using biometrics or a PIN.
- **Reduced costs**: Password-based authentication can be expensive to manage because of the need for password resets and help desk support.

Windows Hello and Windows Hello for Business are both methods of using biometric gestures, such as fingerprints or face recognition, to sign in to Windows devices. However, Windows Hello for Business is configured by policy and uses key-based or certificate-based authentication, while Windows Hello is unique to the device and can use a password hash.

By default, when you join a Windows device to Microsoft Entra, the device will start Windows Hello provisioning.

To configure the default **Windows Hello for Business** behavior, follow these steps:

1. In the Microsoft Intune admin center, go to **Home Devices** | **Windows** | **Windows enrollment** | **Windows Hello for Business**:

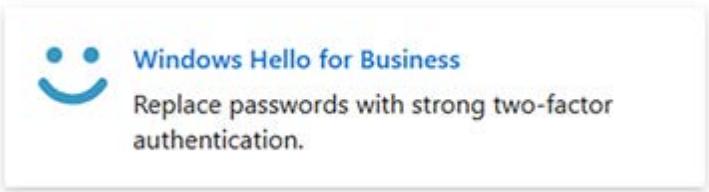


Figure 7.35: Windows Hello for Business

2. By default, in Microsoft Intune, **Configure Windows Hello for Business** is set to **Not configured**, which means that Windows default behavior applies to Windows devices when you are joining to Microsoft Entra – that is, the Windows Hello for Business onboarding wizard will be showed to the end user:

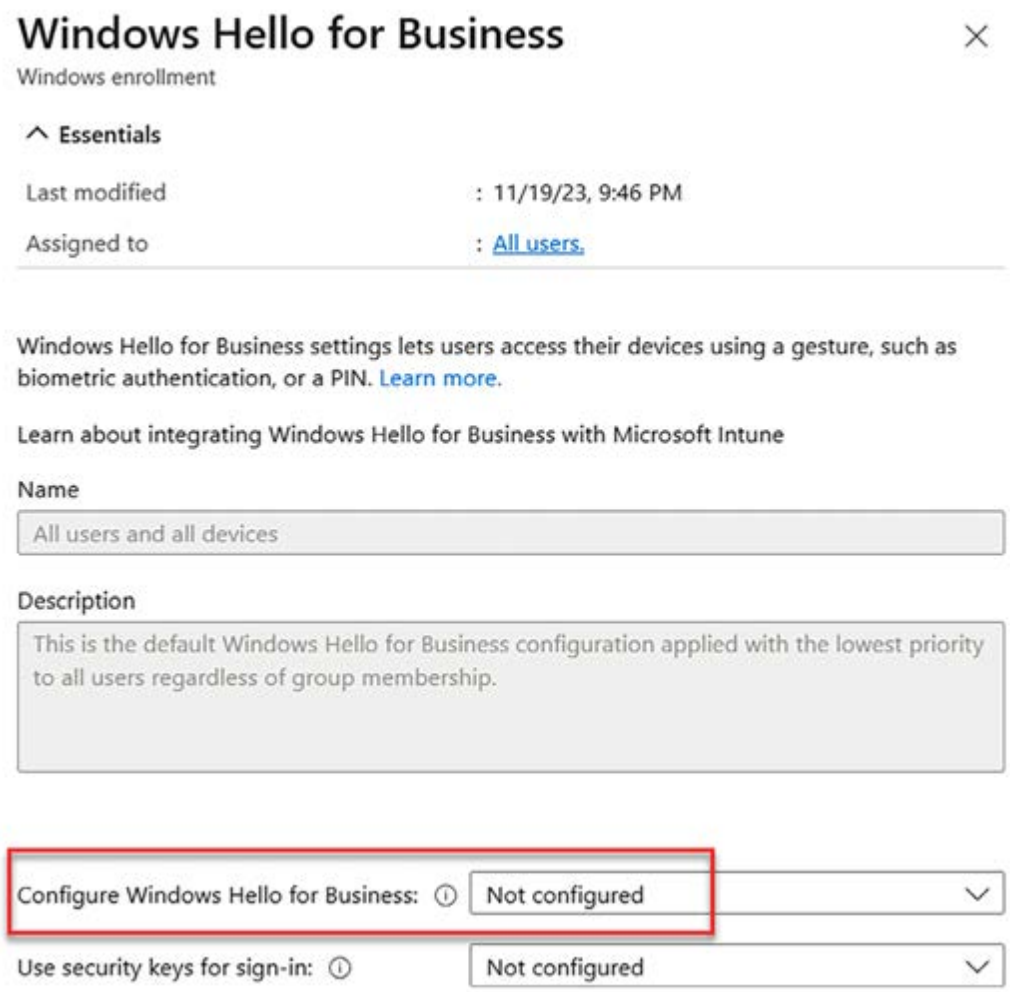


Figure 7.36: Windows Hello for Business default configurations

3. We recommend that you configure the Windows Hello for Business settings so that they match your corporate security policies.



The Windows Hello for Business policy under **Windows enrollment** is tenant-wide – so it applies to every Windows device you enroll into Intune.

4. Let's say that you want to have shared Windows devices for **first-line worker** (**FLW**) scenarios or Kiosk devices in your environment – then, we have a different recommendation for the tenant-wide policy:

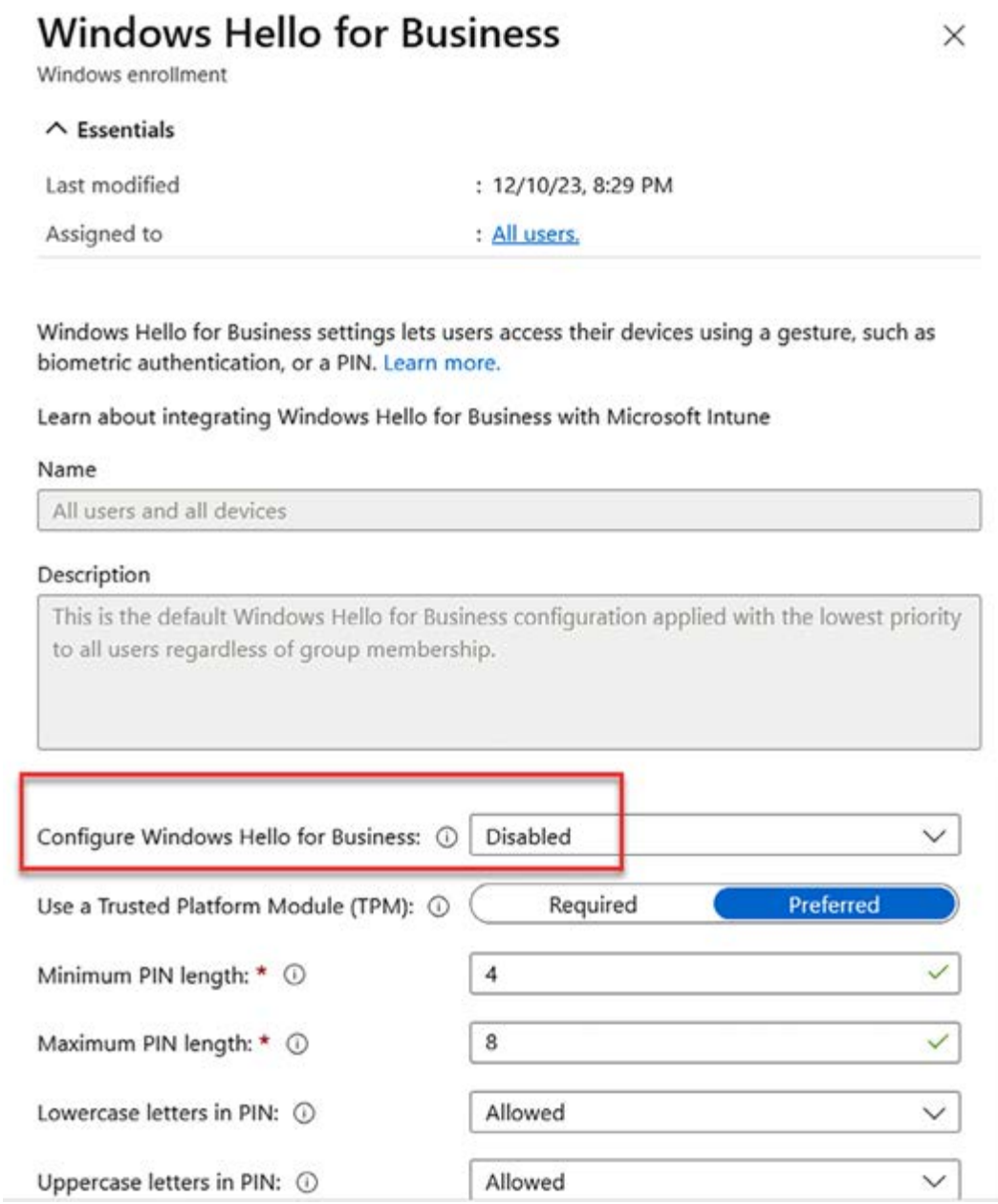


Figure 7.37: Windows Hello for Business: Disabled

So, in scenarios such as the one mentioned above, set **Configure Windows Hello for Business** to **Disabled.**

However, this also means if you want to leverage Windows Hello for Business in your environment, you need to create a separate policy that enables it and configure the Windows Hello for Business setting you need.

To configure the **Elevation setting** policy, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Endpoint security** | **Account protection** and **Create profile**:

   - **Profile type**: Select **Account Protection**.
   - **Name**: `Account Protection`

   Configure the following settings so they match your requirements:

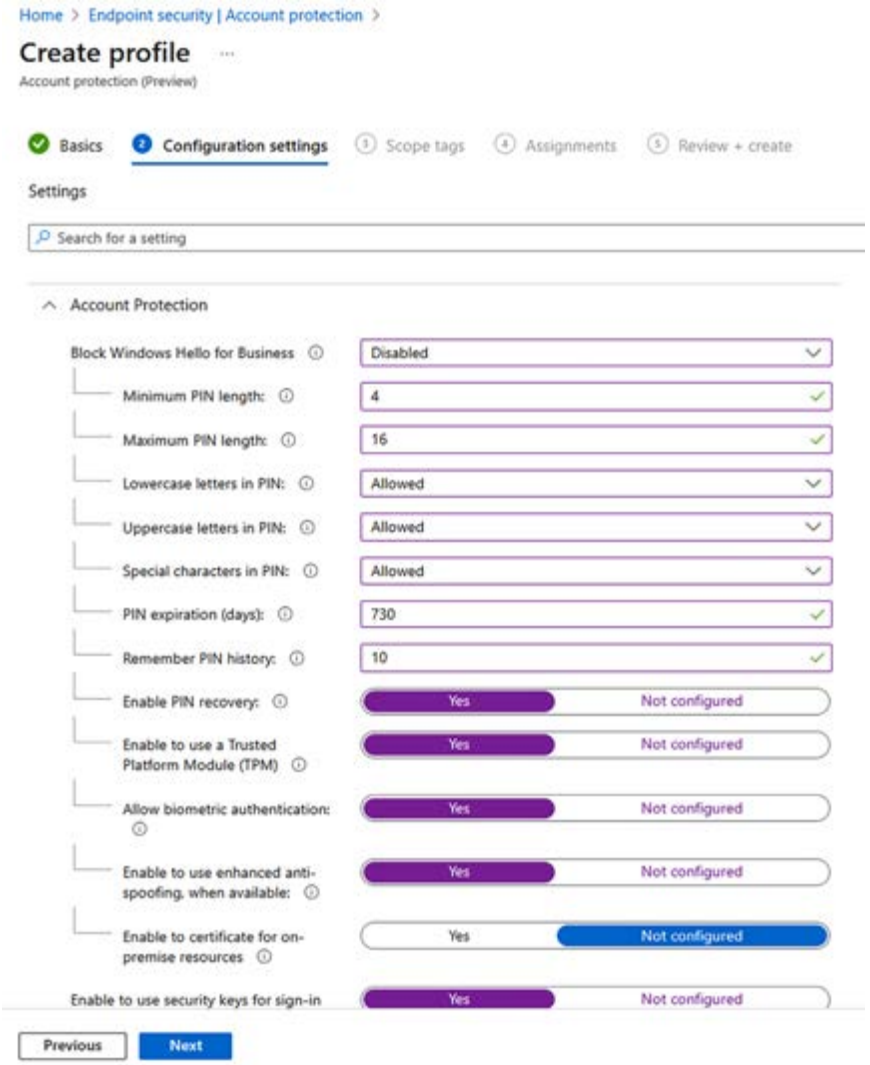


Figure 7.38: Account Protection

2. Assign the policy to your Autopilot device group so the policy applies before the end user signs in to the device for the first time.
3. In the **Account Protection** policy, you can also turn on Credential Guard – the most secure option is **Enable with UEFI lock**:



Figure 7.39: Credential Guard

4. Credential Guard is a Windows Enterprise feature.



From Windows 11 23H2, Credential Guard is enabled by deault on newly installed devices – however, it is not on upgraded devices. Credential Guard has also changed behavior in Windows 11 22H2; if a Windows Enterprise version is downgraded to Pro and has Credential Guard enabled, it will remain enabled.

Cloud configuration scenario

You can leverage deploying Windows 10/Windows 11 in a cloud configuration. In the Microsoft Intune admin center at `https://intune.microsoft.com/`, choose **Troubleshooting + support | Guided scenarios (preview)**:

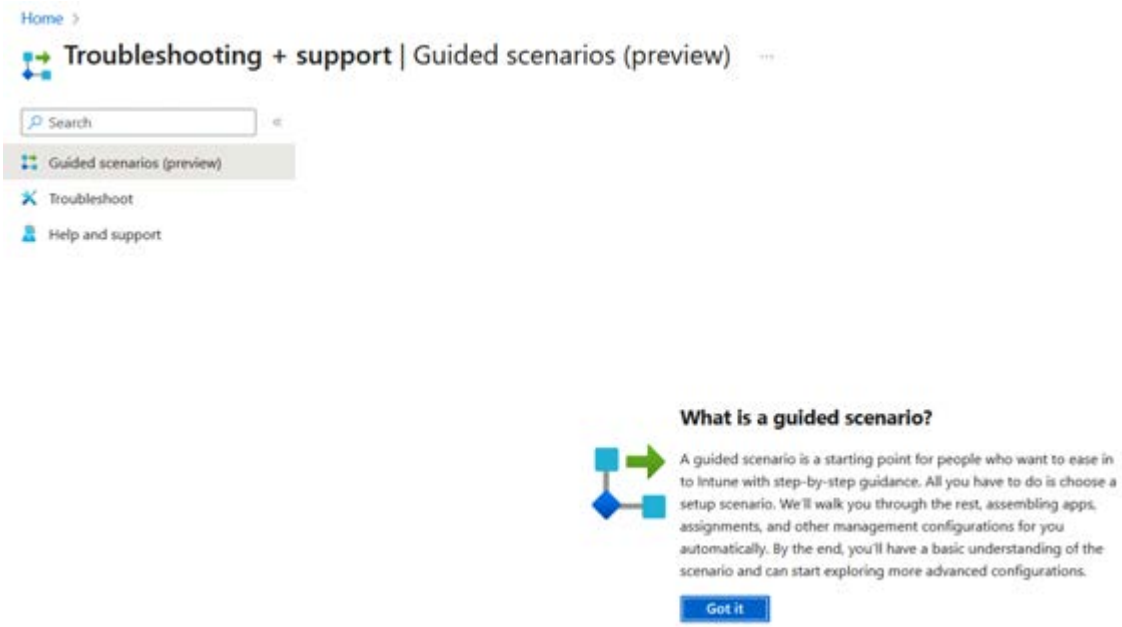


Figure 7.40: What is a guided scenario?

Optimize your Windows devices for the cloud with a simple, secure, standardized configuration fit for your needs:

1. Select **Start** in the **Deploy Windows 10 and later in cloud configuration** guided scenario.
2. In the introduction, select **Next.**

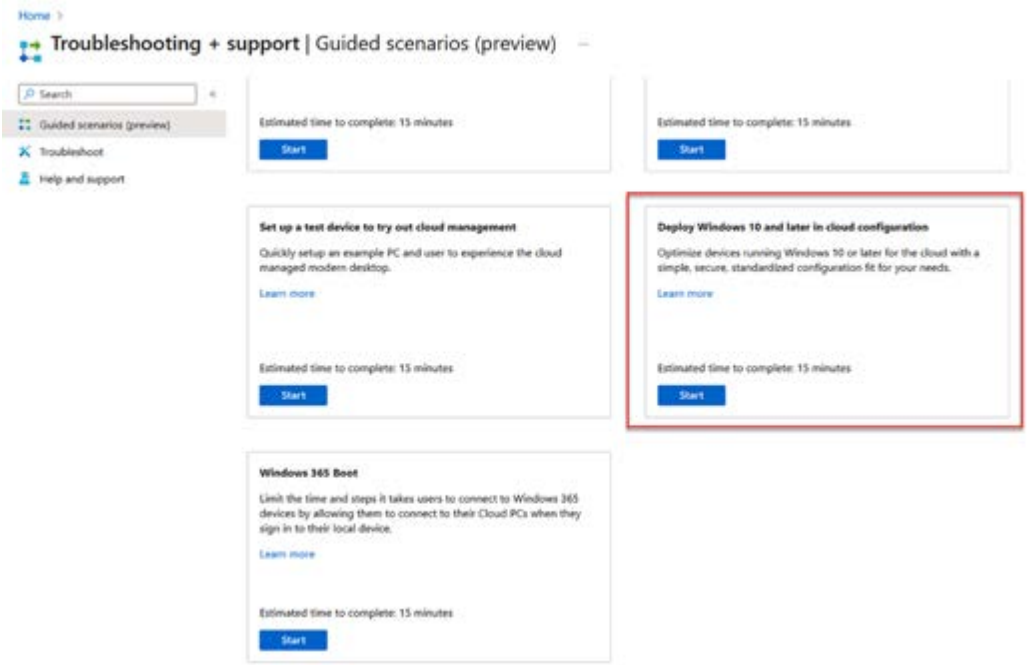


Figure 7.41: Guided scenarios

Introduction

Windows 10 and later in cloud configuration helps to standardize and simplify device management for users with focused workflow needs. You can use cloud configuration to configure new devices or to repurpose and extend the life of existing hardware. It works on any Windows 10/11 Pro, Windows 10 Enterprise, or Windows 10 Education device. Let's now learn more and evaluate the cloud configuration.

The following guided workflow makes it easy to deploy the recommended apps and device configurations found in the cloud configuration overview and setup guide.

Who is this configuration useful for?

Windows in cloud configuration is designed for device users with simplified needs, such as productivity and browsing. Ideal candidates are groups of users in your organization who:

- Use a focused set of apps curated by IT for their workflow needs, like email, Microsoft Teams, a browser, and essential productivity and line-of-business apps. Apps can be delivered directly to the device or through virtualization.
- Have no dependency on an on-premises infrastructure to be successful in their role.
- Use devices that do not require complex settings configurations or custom agents.

As an admin, you get to enjoy the benefits of a standardized device configuration applied across the organization, simplifying management, troubleshooting, and device replacements.

End users enjoy a familiar Windows 10/11 experience optimized for the cloud with just the apps and settings they need.

What you will need to continue

Make sure you have enabled automatic enrollment. You can manage automatic enrollment settings under **Devices** | **Windows** | **Windows enrollment** | **Automatic enrollment**.

Basics

This is where you configure Windows Autopilot settings specific to this scenario:

1. For **Apply device name template**, select **Yes**.
2. Enter a name for the Autopilot name template, such as `Win-%RAND:5%`.
3. Enter a resource prefix name, such as `CloudConfiguration`.

For **Default File Format**, select **Office Open XML**:

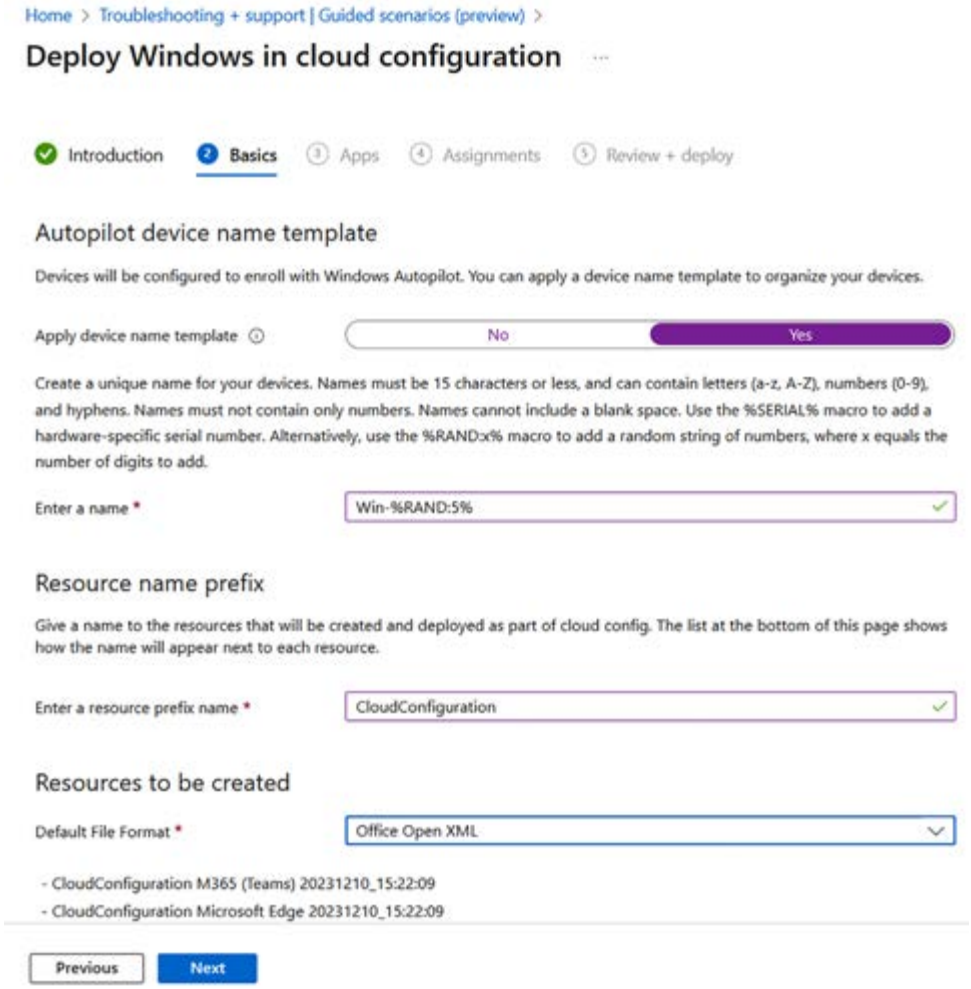


Figure 7.42: Cloud configuration basics

Resources to be created

All these profiles will have the prefix selected:

- `CloudConfiguration M365 (Teams)`
- `CloudConfiguration Microsoft Edge`
- `CloudConfiguration security baseline`
- `CloudConfiguration Autopilot profile`
- `CloudConfiguration ESP`
- `CloudConfiguration OneDrive Known Folder Move settings`
- `CloudConfiguration Microsoft Edge app settings`

- `CloudConfiguration compliance policy`
- `CloudConfiguration built-in app removal script`
- `CloudConfiguration update ring`

Apps

This is the section where you choose the apps you want to deploy as part of the cloud configuration scenario.

Go to **Select additional M365 apps (optional)** | **Outlook** and add other apps if they need to be installed on the device:

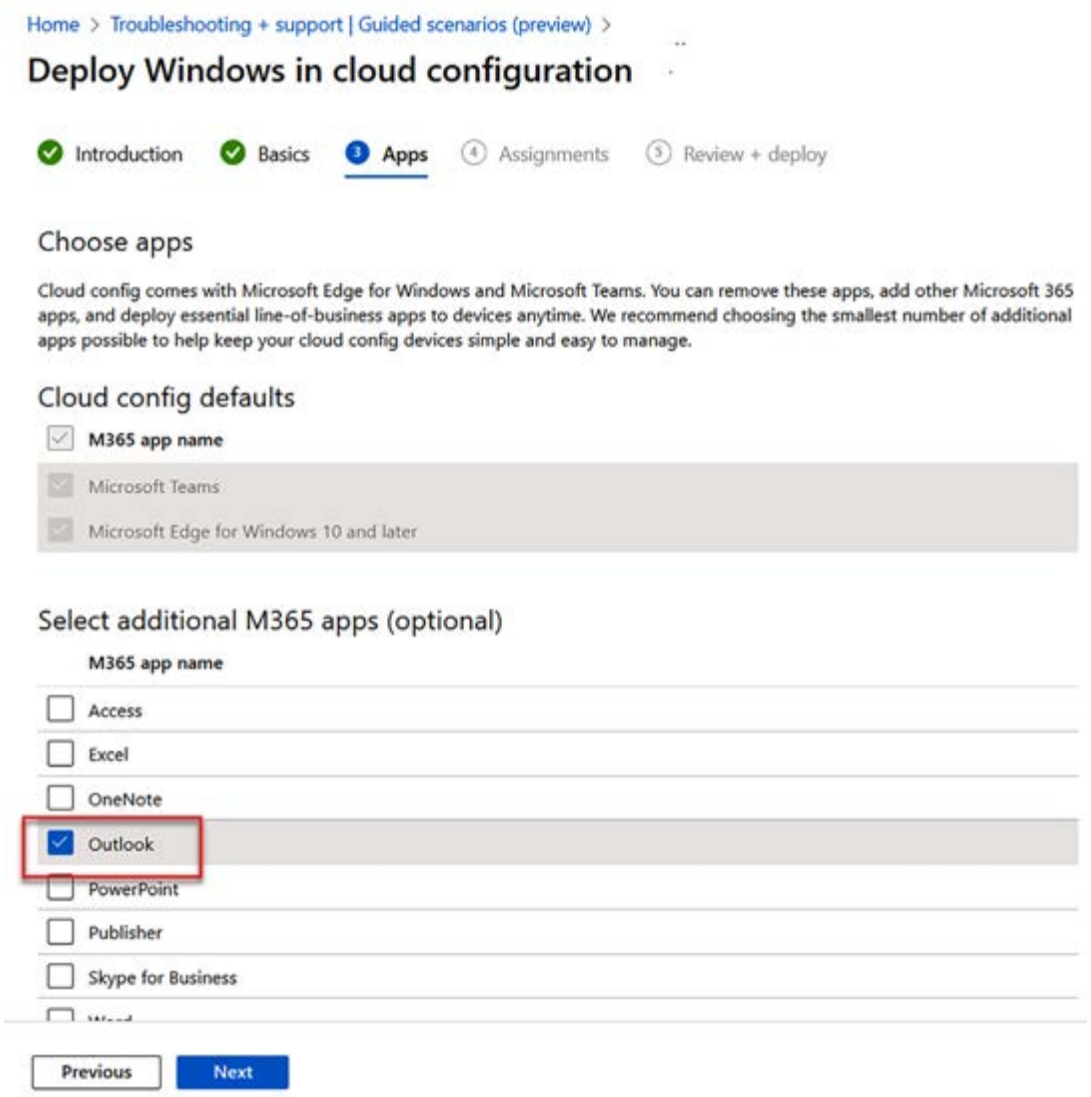


Figure 7.43: Cloud configuration apps

Assignments

Select **Create a new group** and, for **Group name**, enter `CloudConfiguration`.

This will create an empty group so you can put devices in that group and test the deployment as necessary:

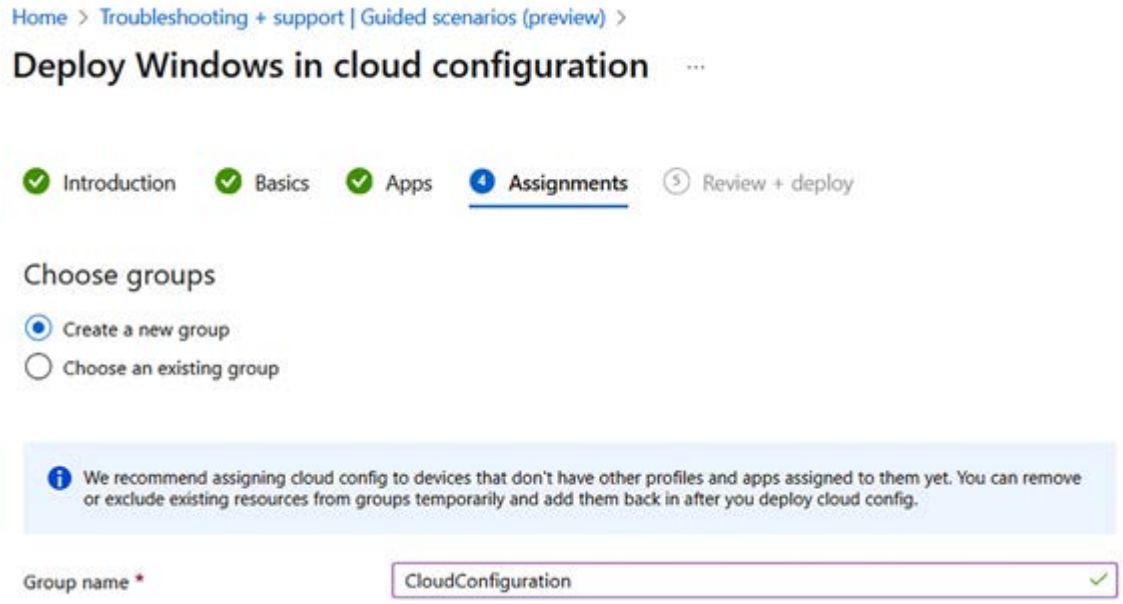


Figure 7.44: Cloud configuration assignments

Deploying

Review your settings in the summary and select **Deploy:**

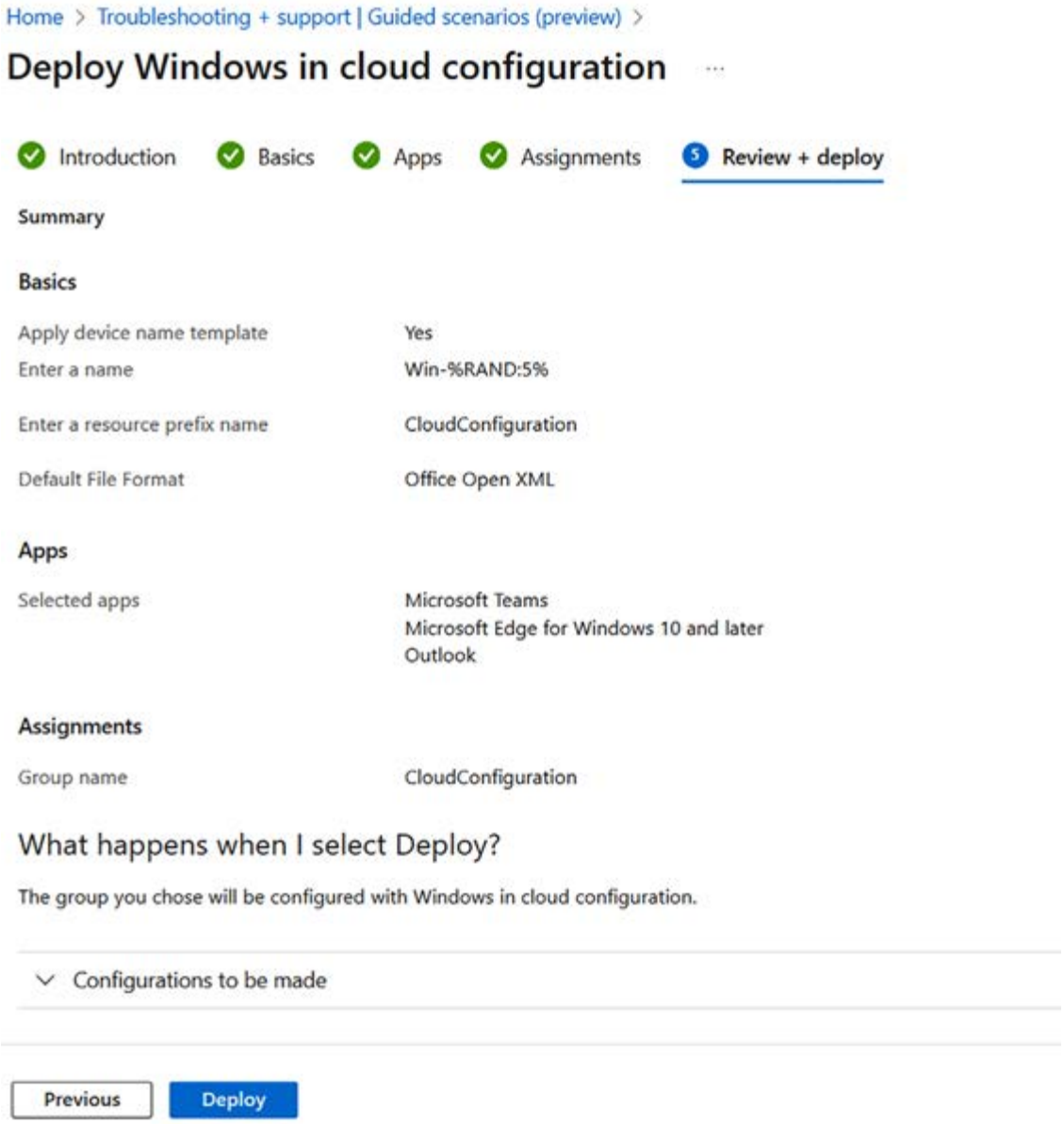


Figure 7.45: Cloud configuration Review + deploy

All the profiles will now be created:

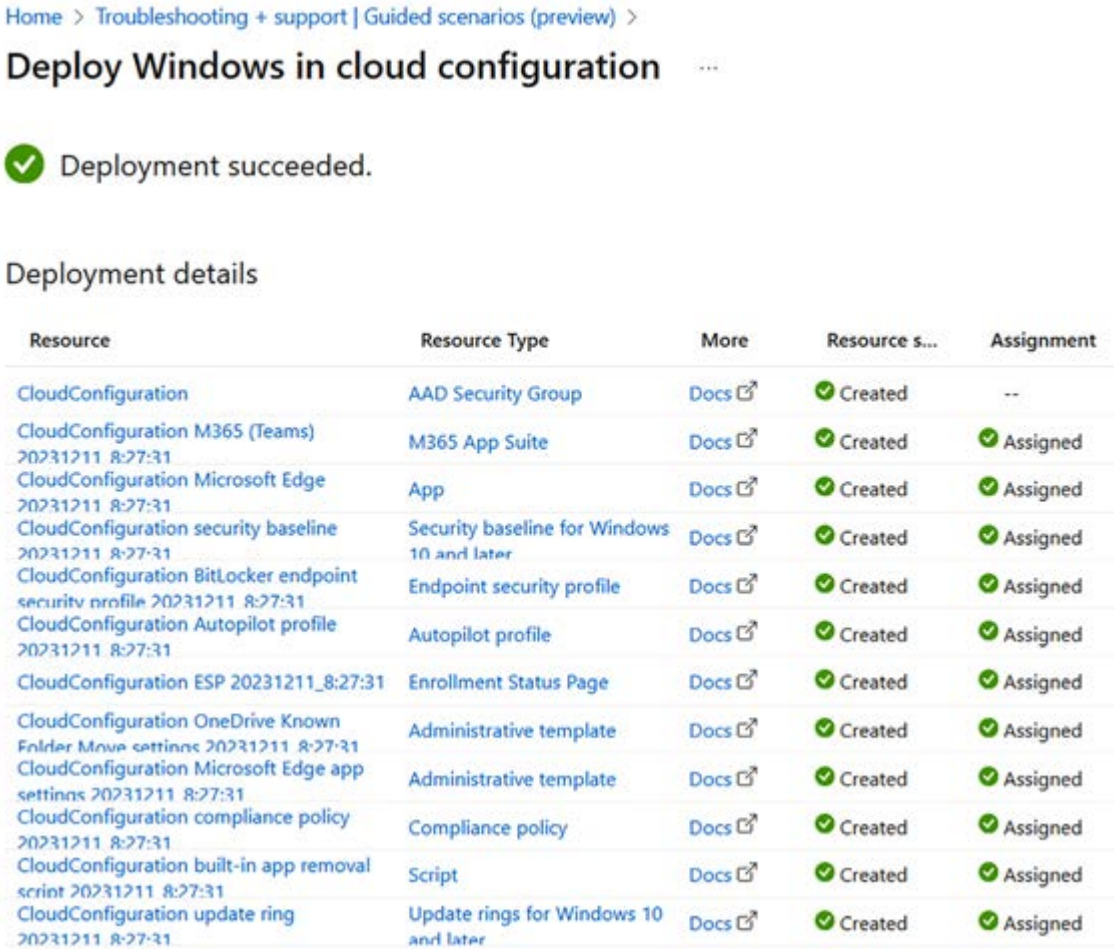


Figure 7.46: Cloud configuration deployment succeeded

Here is what can you do next:

1. Add devices to the group you configured.
2. Add your preregistered Autopilot devices or other existing devices to the group you configured. For existing devices, we recommend removing other profiles and apps and resetting them, so they start fresh with just the cloud configuration applied.
3. Deploy essential line-of-business apps and configurations.

We recommend keeping additional essential configurations to a minimum, including the number of line-of-business apps you deploy on top of the cloud configuration. This helps keep device management and troubleshooting simple.

Deploying essentials that users might need to access work or school resources

Be sure to configure the certificates, VPN profiles, Wi-Fi profiles, and desktop/app virtualization clients that enable access to your organization's resources.

Monitoring your cloud configuration devices

Use Microsoft Intune to monitor the deployment status and device health of your cloud configuration devices.

This is an easy way to start testing Windows Autopilot and cloud-configured devices. In the next section, we will cover how to deploy devices running in Kiosk mode that are being provisioned by Windows Autopilot.

SharedPC self-deployment scenario

Windows SharedPC mode is a feature that optimizes Windows devices for multiple users and guests. It enables settings such as automatic account management, guest and Kiosk accounts, and power and maintenance policies. It also improves the reliability and performance of shared devices. You can configure Windows SharedPC mode using Microsoft Intune, provisioning packages, or PowerShell scripts:

1. Upload Autopilot devices with a group tag such as SharedPC.
2. Create a specific ESP for the SharedPC device.
3. Create a Windows Autopilot profile.
4. Create a SharedPC profile.

Creating a specific ESP for the SharedPC device

A SharedPC device is a multi-user device, and by using Windows Autopilot self-deploying mode, no user has to sign in when onboarding the device into Entra ID or Microsoft Intune, so we will create an ESP and assign it to the Autopilot group for this specific scenario.

Create an ESP with the settings you prefer:

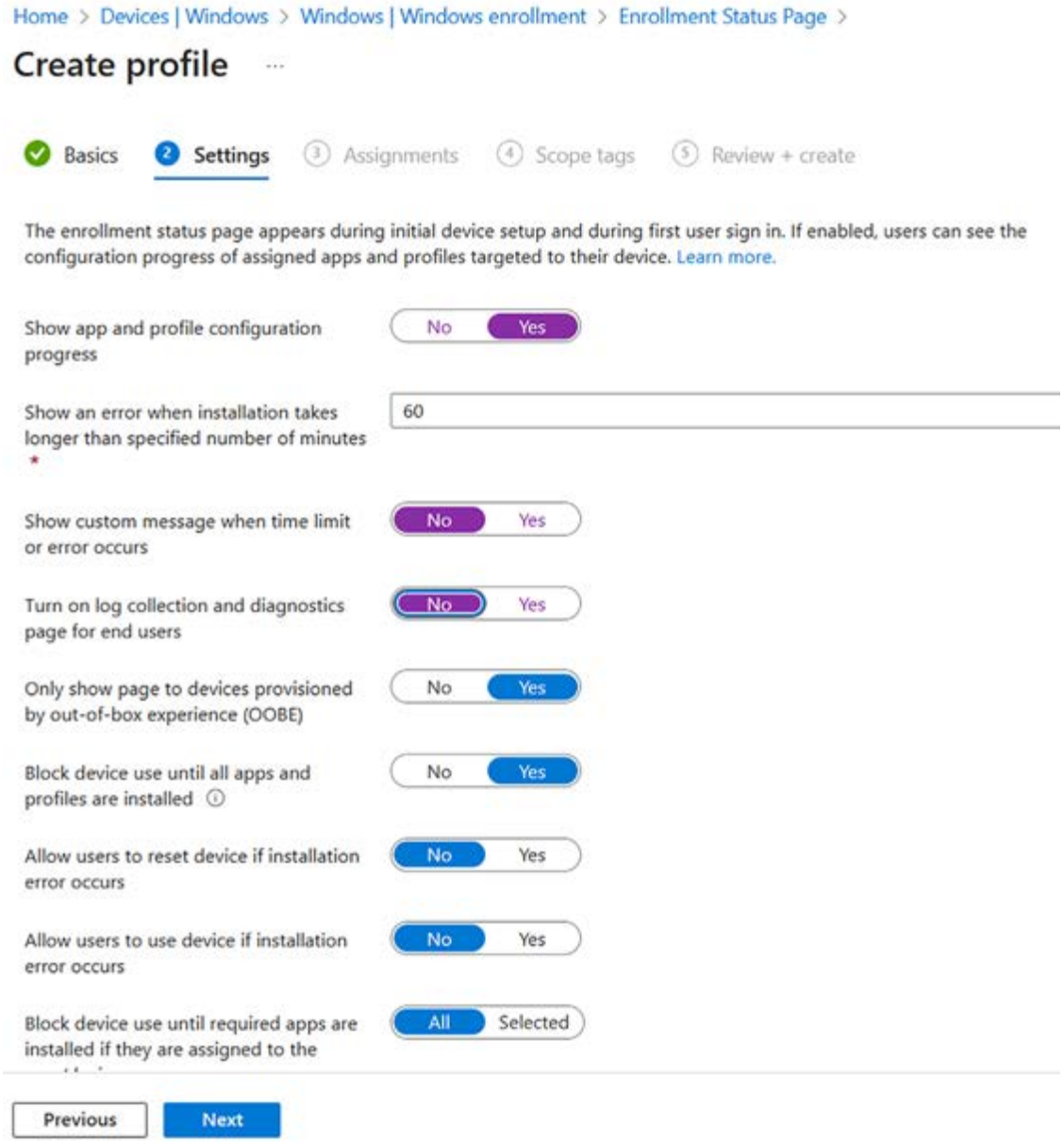


Figure 7.47: Creating an ESP for SharedPC

Assign it to the Entra ID **All Autopilot SharedPC** dynamic group, which will disregard the default ESP profile as it is assigned to a device group. ESP profiles have priority, so be sure what priority your newly created EPS profile has.

Intune applies profiles in the following order:

- Intune applies the highest-priority profile assigned to the device.
- If no profiles are targeted at the device, Intune applies the highest-priority profile assigned to the user. This only works in scenarios where there's a user. In pre-provisioning and self-deploying scenarios, Intune only applies profiles targeted at devices.
- If no profiles are assigned to the device or user, Intune applies the default ESP profile.

Creating a Windows Autopilot profile

Create a new Autopilot profile specific to this scenario:

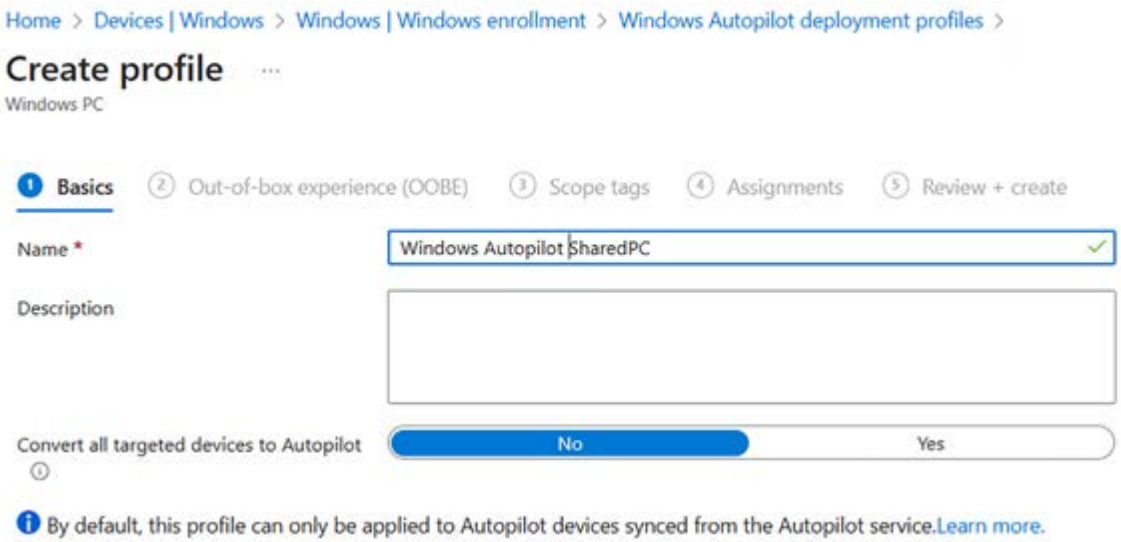


Figure 7.48: Windows Autopilot profile for SharedPC

Set **Deployment mode** to **Self-Deploying (preview)** to onboard the device as a userless device:

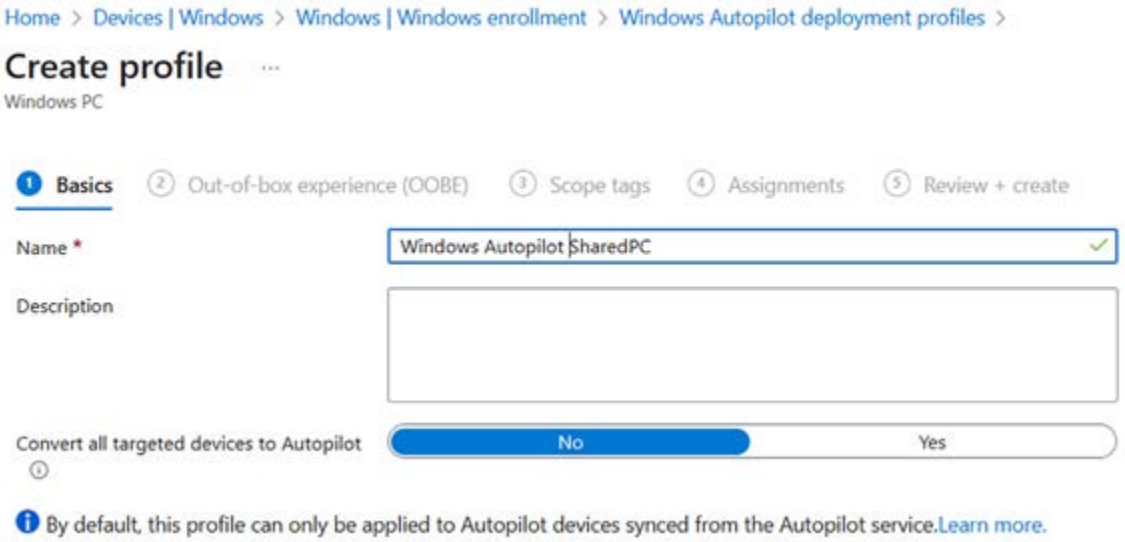


Figure 7.49: Windows Autopilot profile OOBE

Self-Deploying (preview)

The self-deploying mode does not presently associate a user with the device (since no user ID or password is specified as part of the process).

Self-deploying mode uses a device's TPM 2.0 hardware to authenticate the device in an organization's Entra ID tenant. Therefore, devices without TPM 2.0 can't be used with this mode. Devices must also support TPM device attestation. This Windows Autopilot scenario will require a device with a physical TPM, so a virtual device will not work.

To achieve a 100% zero-touch onboarding experience, an Ethernet connection is required; otherwise, the device will prompt you for a region and keyboard layout.

Creating a custom Windows profile to disable user ESP

This is to ensure that the user portion of the ESP will not show up on the EdgeKIOSK as it is a userless device:

- **Name: Disable User ESP**
- **Description: Disable User ESP for EdgeKIOSK**
- **OMA-URI:** `./Vendor/MSFT/DMClient/Provider/ProviderID/FirstSyncStatus/SkipUserStatusPage`
- **Data type: Boolean**
- **Value: True**

Creating a custom Windows 10 profile to disable FirstLogonAnimation

This policy setting allows you to control whether users see the first sign-in animation when signing in to the computer for the first time. This applies to both the first user of the computer who completes the initial setup and users who are added to the computer later. It also controls whether Microsoft account users are offered the opt-in prompt for services during their first sign-in.

If you do not configure this policy setting, the user who completes the initial Windows setup will see the animation during their first sign-in. If the first user has already completed the initial setup and this policy setting is not configured, new users signing in to this computer will not see the first logon animation.

In this EdgeKIOSK scenario, we just want a fast and easy onboarding experience:

- **Name: Disable FirstLogonAnimation**
- **Description: Disable FirstLogonAnimation for EdgeKIOSK**
- **OMA-URI:** `./Device/Vendor/MSFT/Policy/Config/WindowsLogon/EnableFirstLogonAnimation`
- **Data type: Integer**
- **Value: 0**

Creating a Windows template SharedPC profile

Configure Windows to be set up in SharedPC mode. We are using the built-in profile type template with the template name **Shared multi-user device** in Microsoft Intune. This profile type will guide you through the necessary configuration steps. You can always add more policies by adding a settings catalog policy with additional settings.

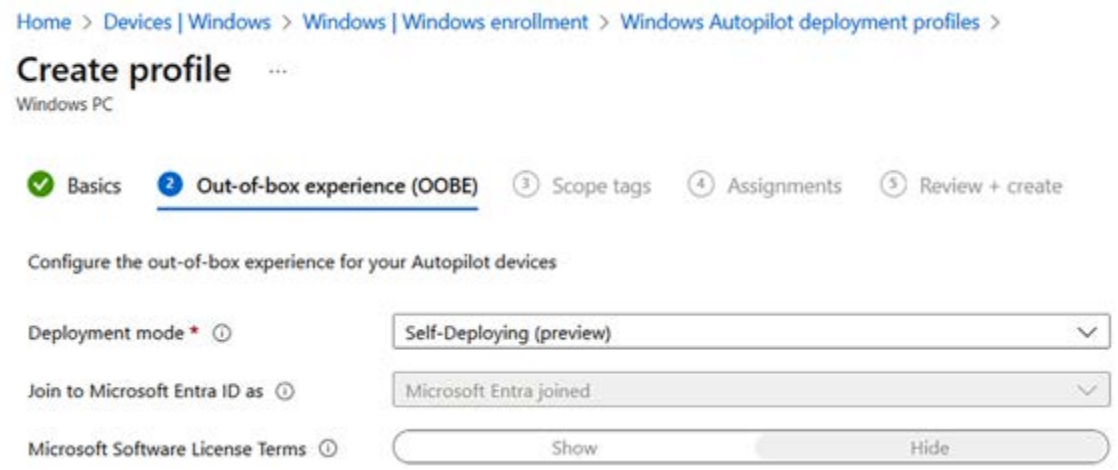


Figure 7.50: Shared multi-user device profile

The following are the settings on the **Configuration settings** tab:

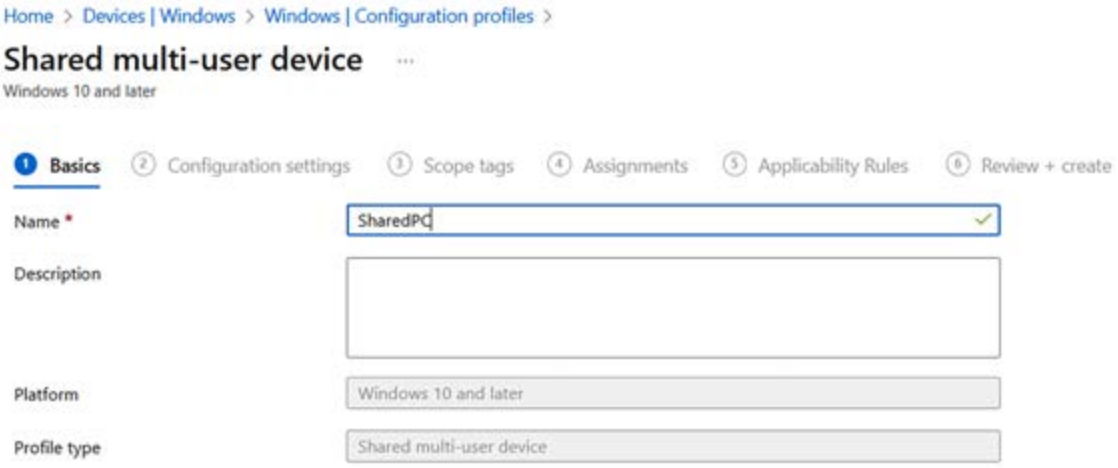


Figure 7.51: SharedPC mode Configuration settings

Configure the following settings:

- **SharedPC mode: Enable**
- **Start delete threshold(%): 25**
- **Stop delete threshold(%): 75**
- **Inactive account threshold: 30**

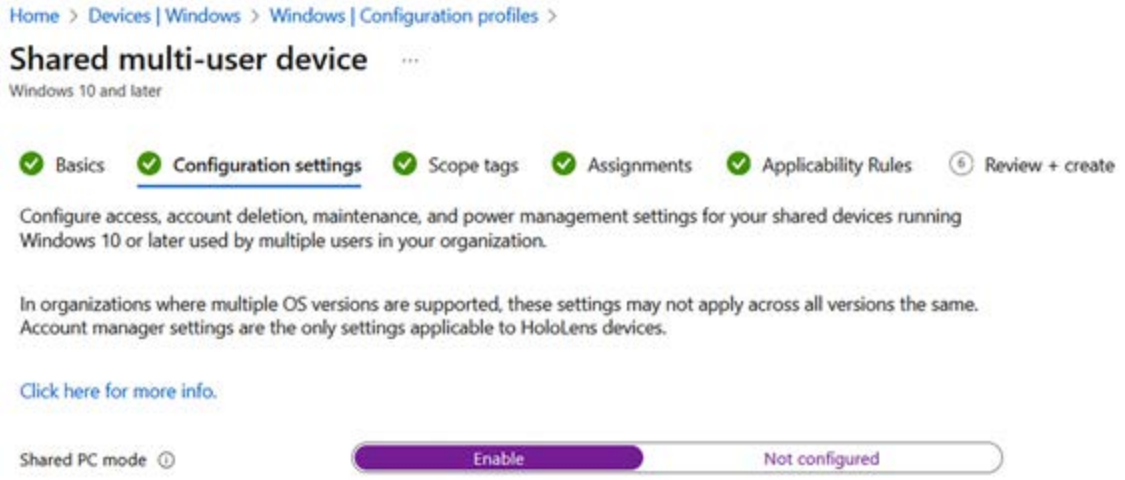


Figure 7.52: SharedPC mode Configuration settings

- **Local Storage: Disabled**
- **Power Policies: Enabled**
- **Sleep time out (in seconds):** Leave blank
- **Maintenance start time(in minutes from midnight): 180**

You can adjust the start time in this setting by entering a new start time in minutes from midnight – in this case, 180 (that is, 3 A.M.). At that time, the automatic maintenance tasks will run, such as Windows Update.

SharedPC technical reference

In this table, you can see what settings are configured for SharedPC:

Policy setting	Status
Security Settings|Local Policies/Security Options/User Account Control: Behavior of elevation prompt for standard user	**Automatically deny elevation requests**
Security Settings/Local Policies/Security Options/Interactive logon: Don't display last signed-in	**Enabled**

Control Panel/Personalization/Prevent enabling lock screen slide show	Enabled
System/Logon/Block user from showing account details on sign-in	Enabled
System/Logon/Enumerate local users on domain-joined computers	Disabled
System/Logon/Hide entry points for Fast User Switching	Enabled
System/Logon/Show first sign-in animation	Disabled
System/Logon/Turn off app notifications on the lock screen	Enabled
System/Logon/Turn off picture password sign-in	Enabled
System/Logon/Turn on convenience PIN sign-in	Disabled
Windows Components/App Package Deployment/Allow a Windows app to share application data between users	Enabled
Windows Components/Biometrics/Allow the use of biometrics	Disabled
Windows Components/Biometrics/Allow users to log on using biometrics	Disabled
Windows Components/Biometrics/Allow domain users to log on using biometrics	Disabled
Windows Components/Data Collection and Preview Builds/Disable pre-release features or settings	Disabled (all experimentations are turned off)
Windows Components/Data Collection and Preview Builds/Do not show feedback notifications	Enabled
Windows Components/Data Collection and Preview Builds/Toggle user control over Insider builds	Disabled
Windows Components/File Explorer/Show lock in the user tile menu	Disabled
Windows Components/File History/Turn off File History	Enabled
Windows Components/OneDrive/Prevent the usage of OneDrive for file storage	Enabled if using EnableSharedPCMode Disabled if using EnableSharedPCModeWithOneDriveSync
Windows Components/Windows Hello for Business/Use biometrics	Disabled
Windows Components/Windows Hello for Business/Use Windows Hello for Business	Disabled

Windows Components/Windows Logon Options/Sign-in and lock last interactive user automatically after a restart	Disabled

Table 7.2: Settings configured for SharedPC

It is recommended to configure other profiles, such as Windows Defender, Windows Update for Business, and other policies that may be relevant to your SharedPC scenario.

Troubleshooting SharedPC

If you need to troubleshoot the SharedPC configuration, here are some steps to take:

- Check the `C:\Windows\SharedPCSetup.log`.
- Check the registry keys under `HKLM\Software\Microsoft\Windows\CurrentVersion\SharedPC`:
  - The `AccountManagement` key contains settings on how profiles are managed.
  - `NodeValues` contains the values that are set for the features managed by `SharedPC`.

Windows Autopilot Reset

Windows Autopilot Reset is only applicable for Entra ID-joined devices.

Windows Autopilot Reset takes the device back to a business-ready state, allowing the same user or a new user to sign in and get productive quickly and simply. The first user who signs in to the device following Autopilot Reset becomes the new primary user and owner of the device. Windows Autopilot Reset can be initialized from the logon screen of Windows (requires a local admin on the Windows device) or from within Intune on each Intune device that is in the Autopilot service as a device action.

Here is what makes Windows Autopilot Reset so special:

- It removes personal files, apps, and settings.
- It maintains the device's identity connection to Entra ID, so it keeps the same Entra ID object.
- It maintains the device's management connection to Intune, so it keeps the same Microsoft Intune Windows object.

When using Windows Autopilot Reset, the process automatically keeps the following information from the device:

- It keeps the region, language, and keyboard that are configured on the device.
- It keeps the Wi-Fi connection details.
- It provisions packages previously applied to the device.
- A provisioning package is present on a USB drive when the reset process is started.
- It retains Entra ID device membership and Microsoft Intune enrollment information.



The Windows Autopilot Reset process does not support Microsoft Entra hybrid joined devices; a full device wipe is required. When a hybrid device goes through a full device reset, it may take up to 24 hours for it to be ready to be deployed again. You can expedite this request by re-registering the device.

Windows Autopilot Reset will block the user from accessing the desktop until this information is restored, including reapplying any provisioning packages until the Microsoft Intune sync is completed.

Perform the following steps in the Microsoft Intune admin center at `https://intune.microsoft.com/`:

1. Choose **Devices** | **Windows** | **Configuration Profiles**.
2. Choose **Create Profile**.
3. Choose **Platform Windows 10 and Later** and **Profile Type Templates**.
4. Choose **Device restrictions** | **Create**.
5. Enter `Enable Autopilot Reset` as the name.
6. Choose **General** | **Autopilot Reset** | **Allow**:



Figure 7.53: Autopilot Reset

7. Allow users with administrative rights to delete all user data and settings using *Ctrl* + *Win* + *R* at the device lock screen so that the device can be automatically reconfigured and re-enrolled into management.
8. Assign the profile to your Autopilot device group.
9. You, as an IT admin, can also initiate Autopilot Reset directly from a device in Microsoft Intune:

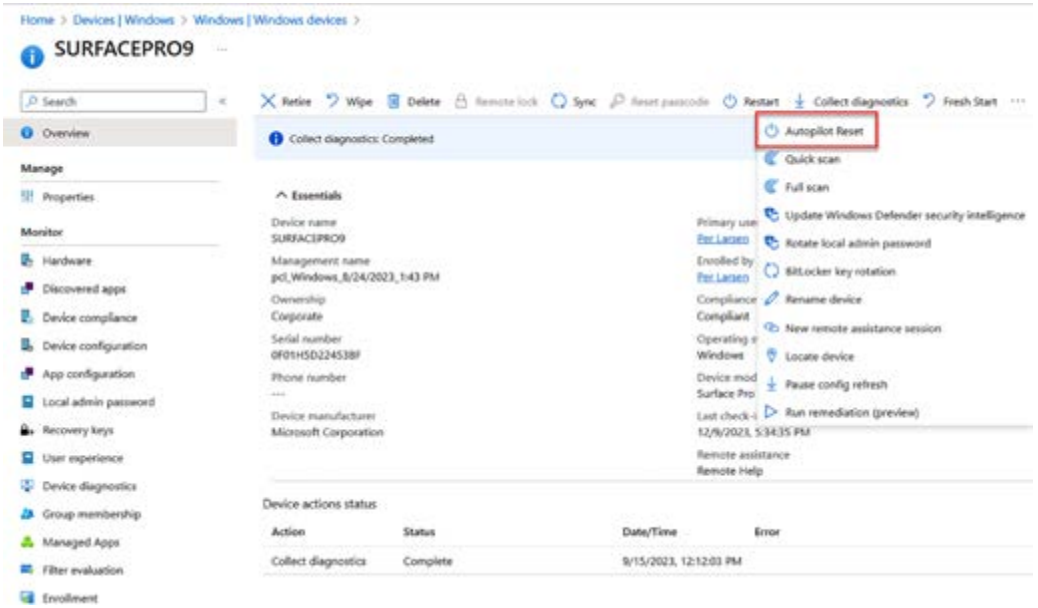


Figure 7.54: Windows device Autopilot Reset

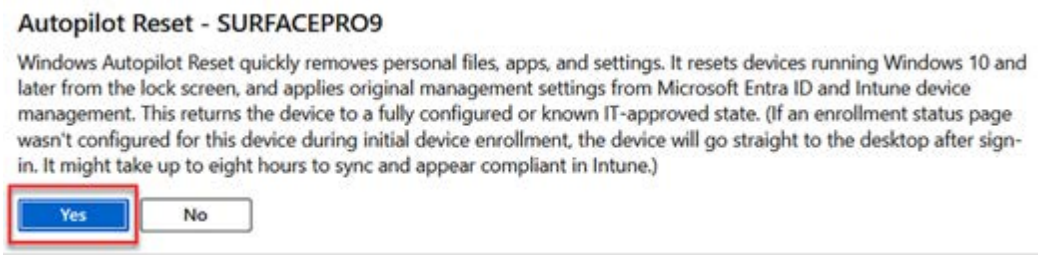


Figure 7.55: Windows device Autopilot Reset additional task

10. As an IT admin, you need to click **Yes** for Autopilot Reset to kick in on the device itself.
11. In the **Device actions status** section, you will see the Autopilot Reset status for whether it has been completed or failed.
12. Other reset scenarios from within Microsoft Intune include those not relying on the device to be a Windows Autopilot device.



If **Windows Defender Application Control** (**WDAC**) is set up to assess app reputation using Microsoft's Intelligent Security Graph, Autopilot Reset may encounter issues, potentially leading to manual reinstallation of the device being required.

Windows Autopilot Reset has a great use case for a device reset if the same user needs to reuse the devices. In the next section, we will cover wiping and resetting.

Wiping and resetting your devices

A factory reset returns the device to its default settings. This removes all personal and company data and settings from the device. You can choose whether to keep the device enrolled and the user account associated with this device. You cannot revert this action.

Are you sure you want to reset this device? Here are the options available to you:

- Wipe device, but keep enrollment state and associated user account:

Retained during a wipe	Not retained
User accounts associated with the device	User files
Machine state (domain-join, AAD-join)	User-installed apps (store and Win32 apps)
MDM enrollment	Non-default device settings
OEM-install apps (store and Win32 apps)	
User profile	
User data outside of the user profile	
User auto logon	

- Wipe device, and continue to wipe even if device loses power. If you select this option, please be aware that it might prevent some Windows 10 devices from starting up again.

This option makes sure that the wipe action can't be circumvented by turning off the device, and will keep trying to reset the device until successful. In some configurations, this action may leave the device unable to reboot.

This issue may be caused when the installation of Windows has major corruption that is preventing the OS from reinstalling. In such a case, the process fails and leaves the system in the Windows Recovery Environment:

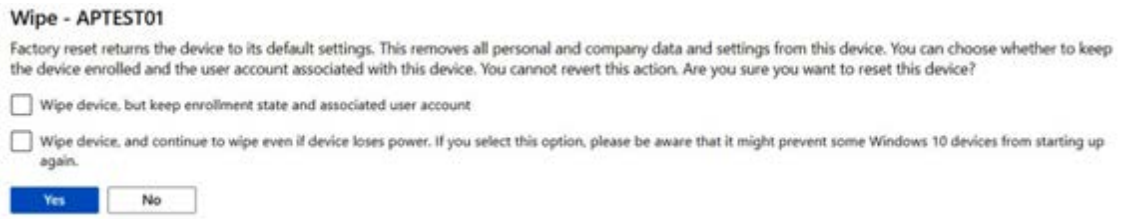


Figure 7.56: Windows device wipe

Fresh Start

Cleaning the device will remove all preloaded Win32 apps. You can choose whether to retain user data on the device and whether you are sure you want to clean the device:



Figure 7.57: Windows Fresh Start

You can also set the following options:

- Keep the device Entra ID joined.
- A device is enrolled in MDM again when an Entra ID-enabled user signs in to the device.
- Keep the contents of the device user's **Home** folder, and remove any apps and settings.



If you do not retain user data, the device will be restored to the default OOBE completed state, retaining the built-in administrator account. That account is disabled by default on Windows Autopilot devices, and you can find yourself in a situation where you are not able to sign in to the device.

Bring Your Own Device (**BYOD**) devices will be unenrolled from Entra ID and MDM. Entra ID-joined devices will be enrolled in MDM again when an Entra ID-enabled user signs in to the device.

Windows Recovery Environment

In many reset scenarios, your devices need to have Windows Recovery Environment enabled. You can check this as follows:

- With **Reagentc/info** in Command Prompt in an administrator context
- With the **Windows Recovery Environment** (**RE**) and a system reset configuration:

```
    Windows RE status:         Enabled
    Windows RE location:       \\?\GLOBALROOT\device\harddisk0\partition4\
Recovery\WindowsRE
    Boot Configuration Data (BCD) identifier: 0d1ee6b6-134c-11eb-abb4-
f32d64eb2b10
    Recovery image location:
    Recovery image index:      0
    Custom image location:
    Custom image index:        0
REAGENTC.EXE: Operation Successful.
```

If the status is **Disabled**, you will need to troubleshoot why the Windows RE is disabled.

Summary

In this chapter, you've learned about Windows Autopilot, including the difference between user-driven and self-deploying modes, how it works, and why it could be beneficial for your organization to simplify the delivery process of your physical endpoints.

We covered what is included in Windows Autopilot device IDs and how to create Entra ID groups based on different attributes to automate different end user scenarios.

We explained what an ESP is, how to configure it, and how to disable the user part of ESP in special scenarios.

In the next chapter, we're going to explain everything concerning application delivery and management via Microsoft Intune.

Questions

1. What is the name of the policy that disables the Windows first logon animation process?
    a. `FirstLogonAnimationExperience`
    b. FirstExperience
    c. FirstLogonAnimation
    d. `WindowsLogonAnimation`

2. What is the default BitLocker encryption method on Windows 11?

    a. AES-CBC 128-bit
    b. XTS-AES 128-bit
    c. AES-CBC 258-bit
    d. XTS-AES 258-bit

Answers

1. (c)
2. (b)

Further reading

If you want to learn more about Windows Autopilot after reading this chapter, please use the following free online resources, and join the Autopilot Microsoft Tech Community!

- *Windows Autopilot | Microsoft Tech Community*: https://techcommunity.microsoft.com/t5/windows-management/windows-autopilot/m-p/90052
- *Windows Autopilot documentation | Microsoft Docs*: https://docs.microsoft.com/en-us/mem/autopilot/
- *Windows AutoPilot: An introduction | Microsoft Tech Community*: https://techcommunity.microsoft.com/t5/windows-deployment/windows-autopilot-an-introduction/td-p/87291

Get This Book's PDF Version and Exclusive Extras

Scan the QR code (or go to packtpub.com/unlock). Search for this book by name, confirm the edition, and then follow the steps on the page.

***Note**: Keep your invoice handy. Purchases made directly from Packt don't require one.*

UNLOCK NOW

8

Application Management and Delivery

In this chapter, you will learn how to deploy and manage your Microsoft 365 and **line-of-business** (**LOB**) applications to your Windows devices, which is a very important element in every Windows Enterprise deployment. Applications are what make end users productive, but applications can also be tools that help either the end user or the IT admin.

In this chapter, we will cover the following topics:

- Application delivery via Microsoft Intune
- Different application types you can deploy
- LOB applications
- Win32 apps
- Deploying Microsoft 365 apps
    - Office Customization Tool
    - Microsoft 365 Apps admin center
- Deploying Microsoft Teams
- Deploying OneDrive
- Deploying Microsoft Edge
- What is WinGet? What is MSIX?

Application delivery via Microsoft Intune

We've been explaining the benefits of using a modern unified endpoint management solution from the same management experience we have covered in the previous chapters of this book. Of course, the same benefits apply to delivering applications to your endpoints, whether they're running Windows Enterprise on a virtual cloud or physical endpoints via Microsoft Intune.

Another important layer is security. Normally, installing apps would require installation rights, such as local administrator permissions on your Windows Enterprise endpoint. Delivering your app via Microsoft Intune allows you to assign and install apps – in a modular fashion – without the need to make the user a local administrator.

Adding applications modularly (separately) from the image would also drastically simplify your image maintenance process. For example, within a legacy virtual desktop infrastructure, you would have created a so-called master image. This is not required with Microsoft Intune as all applications can be managed separately from the OS image layer. After you enroll your Windows Enterprise devices, all your assigned applications are added automatically based on user, group, or device filtering. Sounds pretty cool, right?

To start delivering apps, select the **Apps** menu in Microsoft Intune. You begin your journey of configuring and assigning the application to your users or devices. It's easy, and different application formats are supported, and you will find the explanations for this in this chapter of the book.

Different application types you can deploy

Delivering applications to your end users, whether they are working primarily on a physical or virtual cloud desktop, is a very important factor for enterprises.

Most enterprises have been doing this for years with SMS and Microsoft Configuration Manager (to their on-premises infrastructure and on the internet with the cloud management gateway). Within Microsoft Intune, the process is easier as the backend infrastructure is pre-built to start deploying apps almost immediately!

So, what format of apps are supported as delivery types for each **operating system** (**OS**)? Let's give you a complete rundown so that you can decide what the best approach is for your business.

When you create a new app in Microsoft Intune, you start by selecting an app type that is appropriate for the app you want to deliver to your devices:

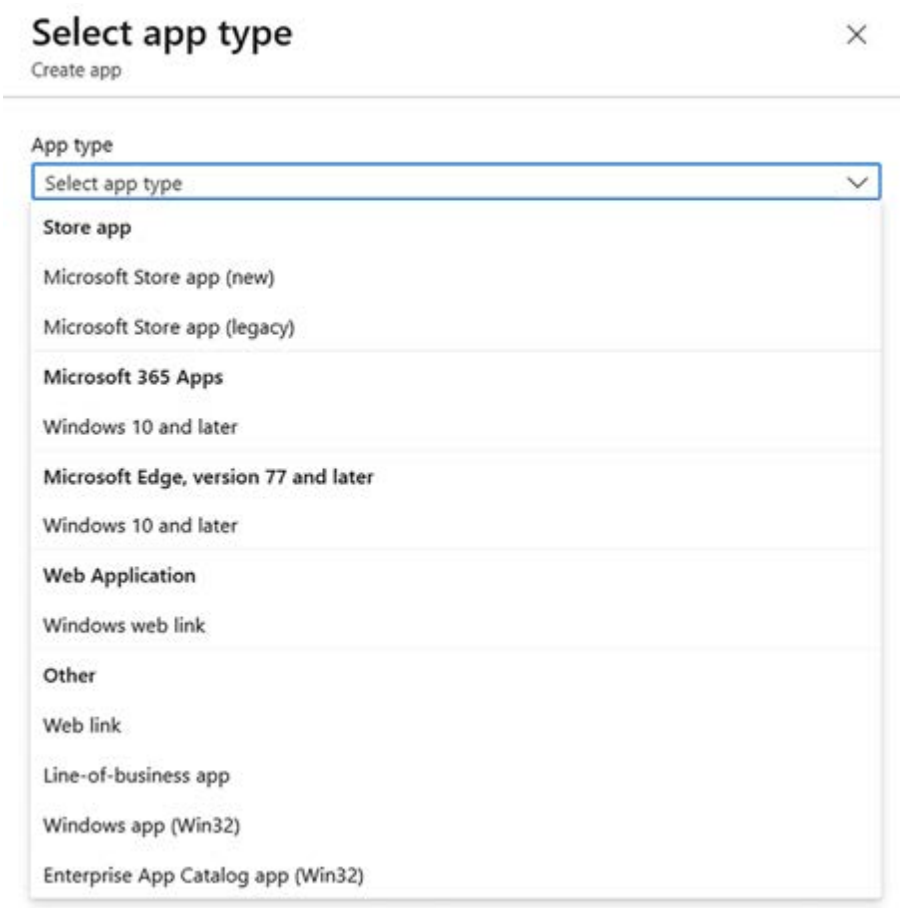


Figure 8.1: Select app type

Supported Windows app delivery types are covered in more detail in the following sub-sections.

LOB applications

Within Intune, you can deploy different formats using different methods. The supported formats are modern apps, such as **Universal Windows Platform** (**UWP**) apps, **Windows App Packages** (**AppX**), and MSIX – via the LOB app as well as more classic formats such as Win32 apps, including simple **Microsoft Installer** (**MSI**) package files.

MSI – via the LOB app

MSI format installers are supported by both the LOB and the Windows app (Win32) options within Intune, with the latter more enhanced for app dependencies.

MSIX – via the LOB app

MSIX is Microsoft's new Windows app package format that provides a modern packaging experience to all Windows apps. The MSIX package format preserves the functionality of existing app packages and/or install files in addition to enabling new, modern packaging and deployment features to Win32, WPF, and Windows Forms apps. We'll go deeper into the MSIX format later on in the book.

MSIX combines the best features of MSI, `.appx`, and App-V.

AppX – via the LOB app

The AppX application distribution file format was first introduced with Microsoft Windows 8. Also known as modern (UWP) apps, files with an AppX extension added are directly ready for distribution and installation.

Within the Windows Store as part of Windows, apps are automatically distributed in the AppX – UWP format.

AppX is very beneficial for distributing applications supported by multiple devices, including PCs, tablets, HoloLens, and Surface Hub.



When you use Autopilot, we recommend that you do not mix LOB apps with the Windows 32 app (Win32) as a delivery option – you can find more information about this in *Chapter 7*, *Windows Autopilot.*

To configure a simple LOB app, while in the Microsoft Intune console, you must go to **Apps** in the menu to start the configuration:

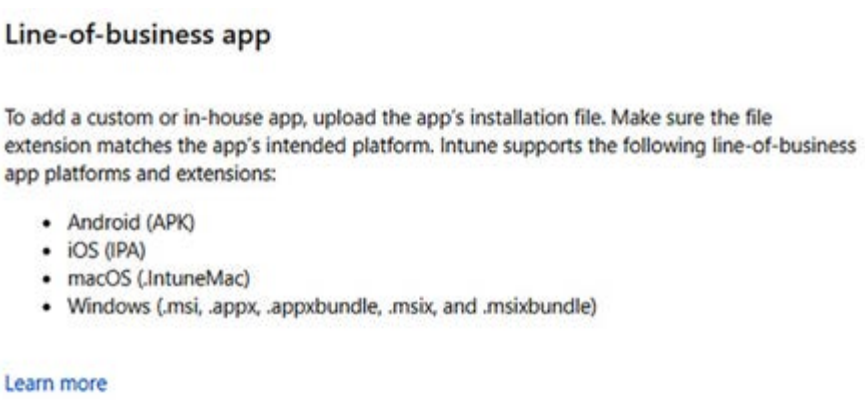


Figure 8.2: LOB app

1. You start the configuration via the **+ Add** button:

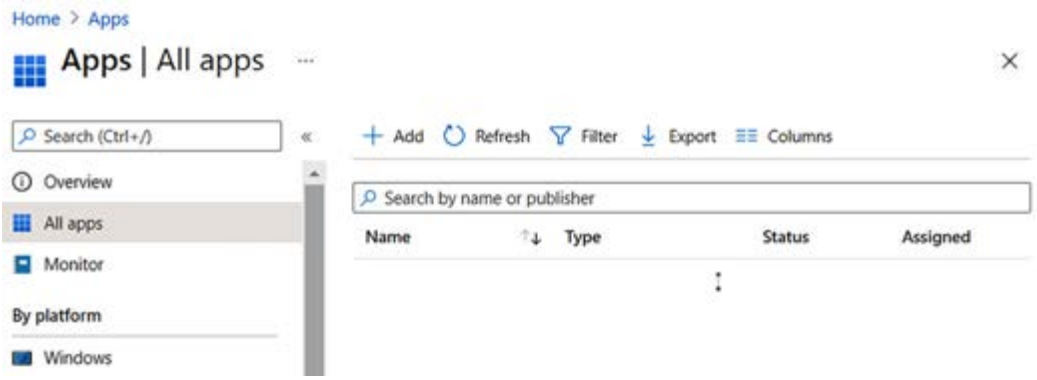


Figure 8.3: All apps

2. The following menu shows all the supported app types, as mentioned previously. To start with the configuration for the most simple way to deploy an MSI file, you select **Line-of-business app**.

   To deploy MSI files and other Win32 application formats in a more advanced manner, we recommend you use the Windows app (Win32) option – explained in the next section.



The Win32 app model supports dependencies and supersedence, whereas LOB apps do not support these options.

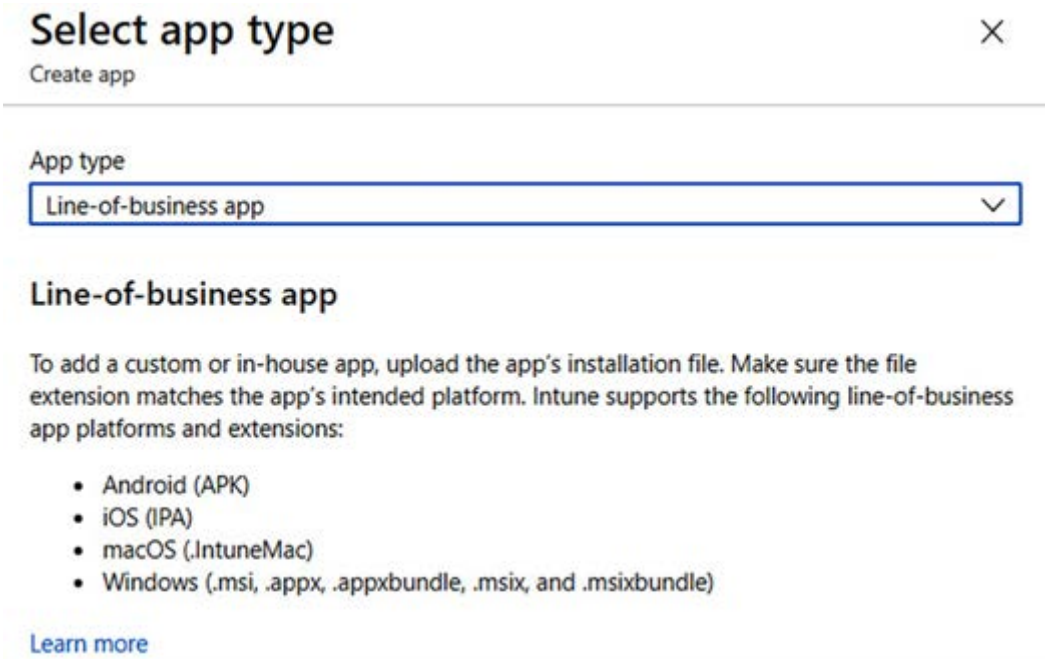


Figure 8.4: App type – Line-of-business app

3. Browse in the file system to the `.msi` file that you want to create the app for (`.exe` isn't supported – please use the Win32 app type for this instead):

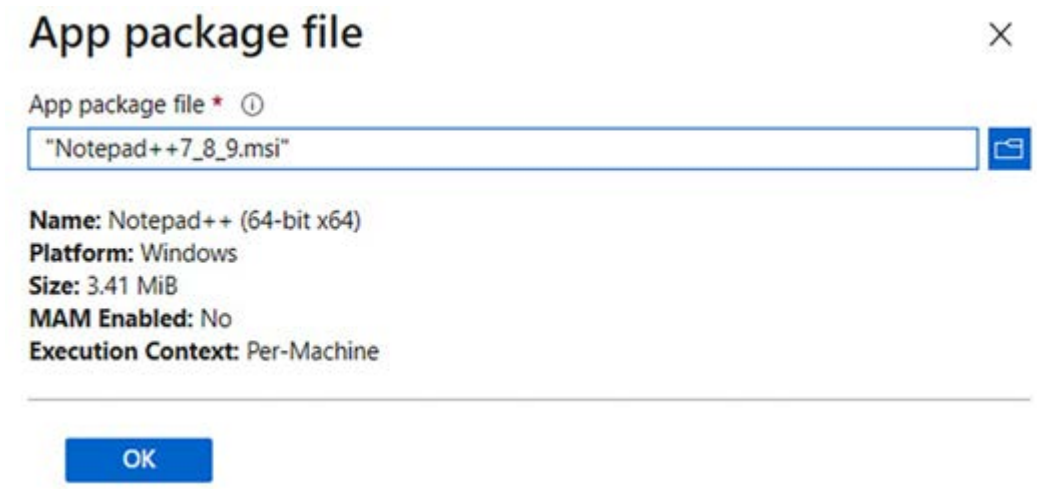


Figure 8.5: App package file

4. Give the LOB application a suitable app name, description, and publisher.
5. There are other optional values that you could select:
    - App installation context (user or device)

- App version ignorance
- Command-line arguments (parameters for the installation)
- Category to define the type of application
- List the application in the Company Portal (or not)

As you can see, limited capabilities are available here.

6. When you need more complex application installation and/or dependencies/supersedes, please use the Win32 app approach:

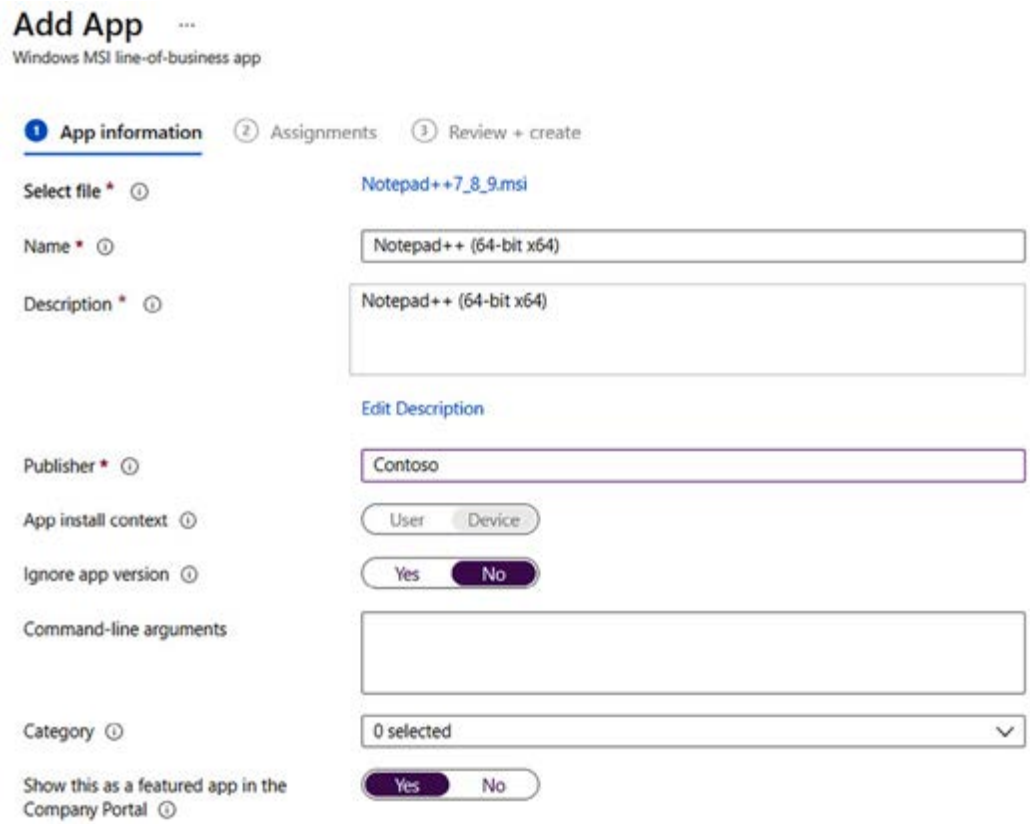


Figure 8.6: Add App – Windows MSI app information

7. Create the suitable Entra ID user, Entra ID device group, or device-based filtering for your Windows MSI LOB app.

8. Start the deployment of the application after you have verified the configuration summary:

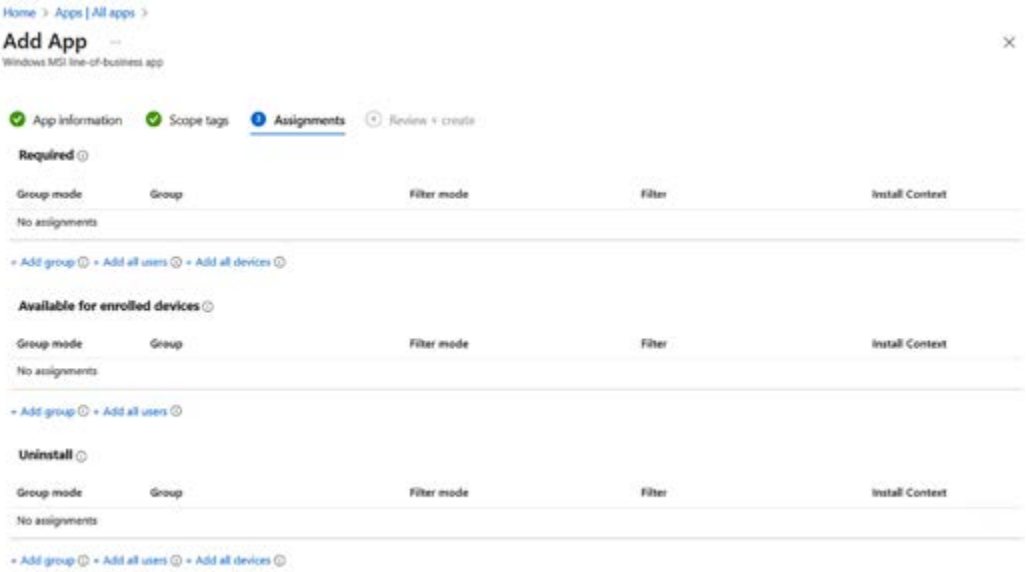


Figure 8.7: Add App – Windows MSI Assignments

9. Enrollment starts directly for the designated users and devices after you see the following prompt in the top right-hand corner of the admin center.
10. Following a successful installation, Notepad++ pops up in the **Start** menu as a new, recently added application:

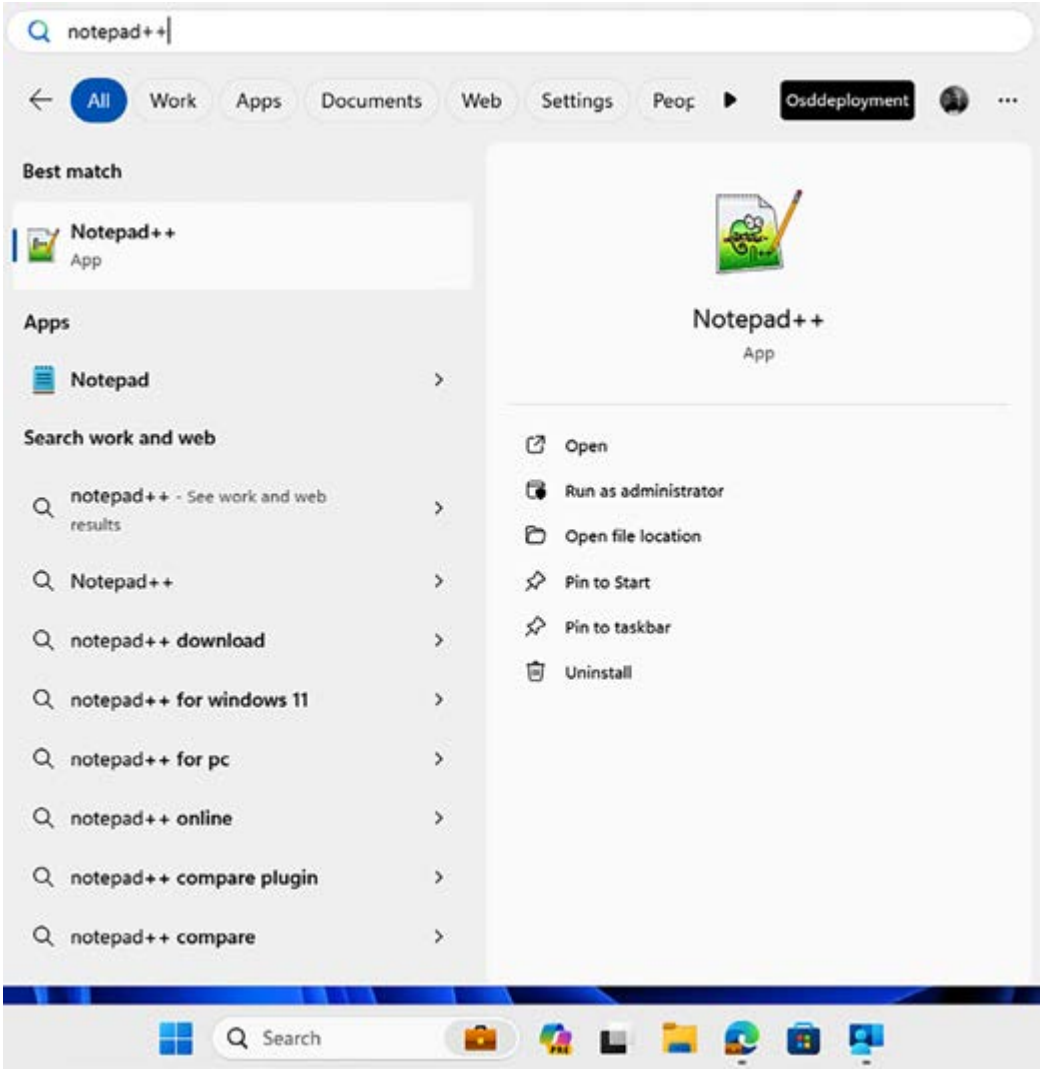


Figure 8.8: Starting the recently added app

Then, the end user can start using the app or pin it to the **Start** menu.

IntuneWin – via the Windows app (Win32)

The IntuneWin format is a way to preprocess Windows Classic (Win32) apps. The tool converts application installation files to the `.intunewin` format.

After you use this tool on the app packaging folder, you'll be able to create an app enrollment configuration that allows enhanced deployment capabilities such as OS version dependencies and uninstallation methods when you need to remove applications remotely.

Win32 apps in Intune have a size limit of 30 GB per app.



Intune will install the Intune Management extension on the device if a PowerShell script or a Win32 app is targeted at the user or device.

When you select the most common application format, which is the Win32 app, you must go through the following process. You have to encapsulate the `.exe` or `.msi` file in an IntuneWin file that we need as part of the app configuration set.

Here are the sample commands to use for the Microsoft Win32 Content Prep Tool:

- `IntuneWinAppUtil –v`
    - This will show the tool version (only available starting version 1.8.2)
- `IntuneWinAppUtil -h`
    - This will show usage information for the tool
- `IntuneWinAppUtil -c <setup_folder> -s <source_setup_file> -o <output_folder> <-q>`
    - This will generate the `.intunewin` file from the specified source folder and setup file
    - For the MSI setup file, this tool will retrieve the required information for Intune
    - If `-a` is specified, all catalog files in that folder will be bundled into the `.intunewin` file
    - If `-q` is specified, it will be in quiet mode. If the output file already exists, it will be overwritten
    - Also, if the output folder does not exist, it will be created automatically
- `IntuneWinAppUtil`
    - If no parameter is specified, this tool will guide you to input the required parameters step by step

Here are additional command-line parameters available for `IntuneWinAppUtil`:

- `-h`: Help
- `-v`: Tool version (only available starting version 1.8.2)

- `-c <setup_folder>`: A setup folder for all setup files. All files in this folder will be compressed into the `.intunewin` file
    - Only the setup files for this app should be in this folder
- `-s <setup_file>`: The setup file (e.g. `setup.exe` or `setup.msi`)
- `-o <output_file>`: The output folder for the generated `.intunewin` file
- `-a <catalog_folder>`: The catalog folder for all catalog files. All files in this folder will be treated as a catalog file for Win10 S mode

Here are the high-level steps of the process flow to understand the process:

1. Select your Win32 application installation file (`.exe` or `.msi`) and create the IntuneWin file as a package.
2. Start the app configuration in **Microsoft Intune | Intune**.
3. Configure the necessary application info, such as the publisher and names.
4. Configure the application details to install the application, such as silent installation and uninstallation parameters.
5. Configure any requirements you have for the application, such as dependencies or the need for a PowerShell script to run before the installation starts.
6. Enable supersedence mode to update the older version of the application (more on this later). This feature is in preview.
7. Configure return code for logging purposes.

To start the configuration and delivery of a Windows 32 application (Win32), you must select the app type as follows:

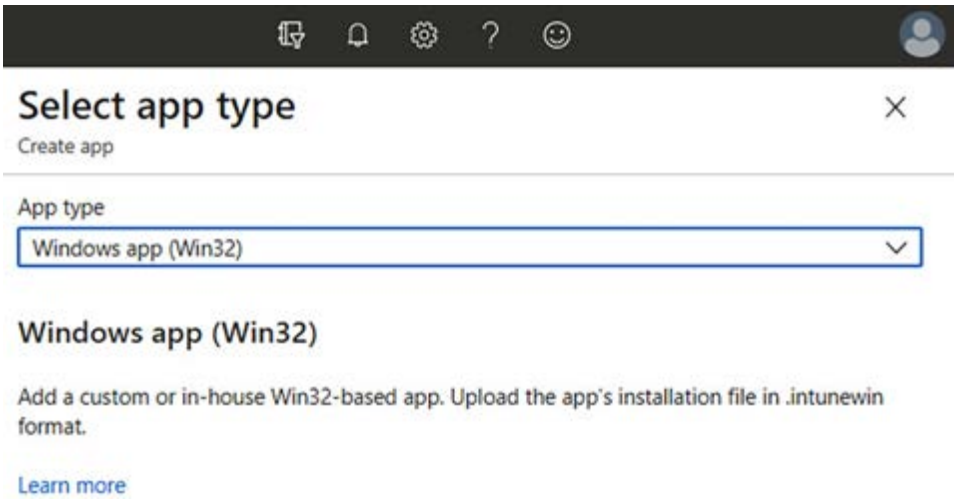


Figure 8.9: Select app type

Add a custom or in-house Win32-based app. Upload the app's installation file in the `.intunewin` format. The following example demonstrates the packaging process for the most famous app used in demos – Notepad++.

The capabilities to filter out and create dependencies are much greater than with the previous LOB approach. The capabilities we use in this section apply to any Win32 application you have. Let's begin:

1. Firstly, download the Microsoft Win32 Content Prep Tool: `https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool`.
2. Unzip the tool, for example, in the `C:\` drive (you could pick a random folder as well).
3. Save your application `.exe` or `.msi` file in, for example, the same folder as the Content Prep Tool (selected previously). It could also be saved somewhere else, of course, and that would mean that the package size would be smaller, so an advantage. *I'm using Notepad++ for this example because it's free*:

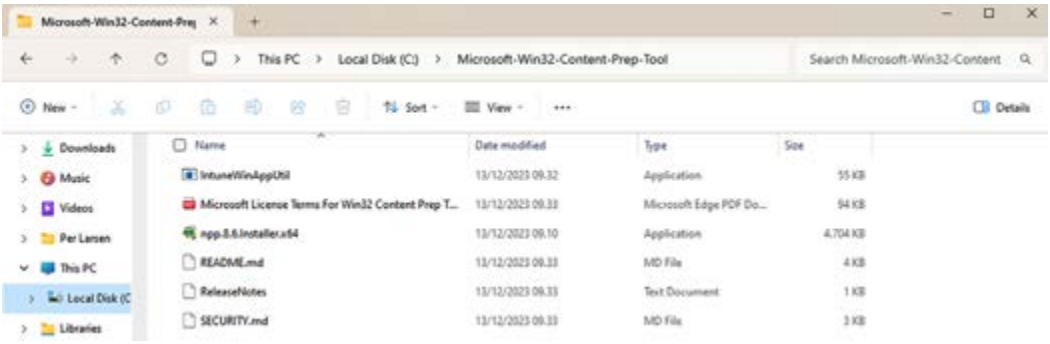


Figure 8.10: Browse for your app

4. Now, we start creating the `Win32.Intunewin` package.
5. Open PowerShell and change the directory to the Content Prep Tool location, for example, `C:\Microsoft-Win32-Content-Prep-Tool-master`:

```
cd "C:\Microsoft-Win32-Content-Prep-Tool-master"
```

This command gives the following output:



Figure 8.11: Win32 Content Prep Tool master

6. Run `.\IntuneWinAppUtil.exe` and fill in the following requirements:
    - `Please specify the source folder: C:\Microsoft-Win32-Content-Prep-Tool-master`
    - `Please specify the setup file: npp.8.6.Installer.x64.exe`
    - `Please specify the output folder: C:\Microsoft-Win32-Content-Prep-Tool-master`
    - `Do you want to specify catalog folder (Y/N)? N`

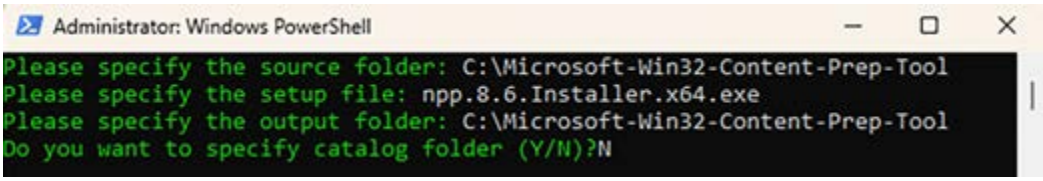


Figure 8.12: IntuneWinAppUtil



You can customize the folders as you like. This is just an example.

7. If everything ran successfully, you will see the `.intunewim` file listed in the folder. We can now switch to Microsoft Intune:

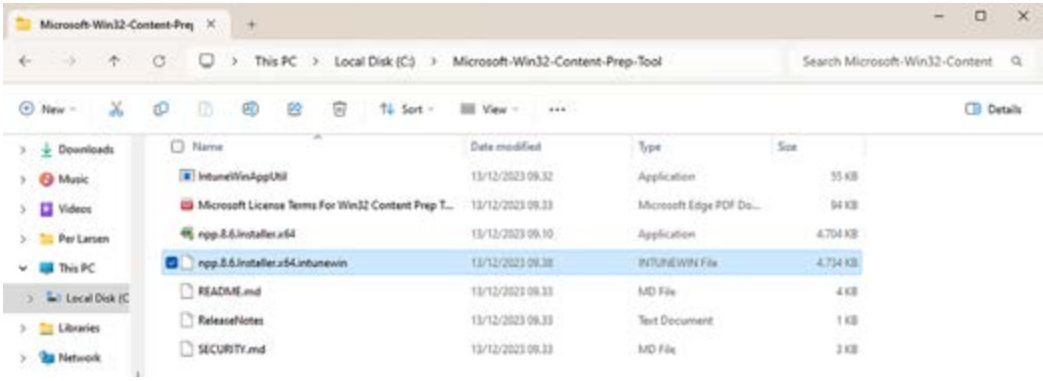


Figure 8.13: .intunewim

8. Go to `http://intune.microsoft.com/` to continue in the Microsoft Intune admin center. Go to the **Apps** field:

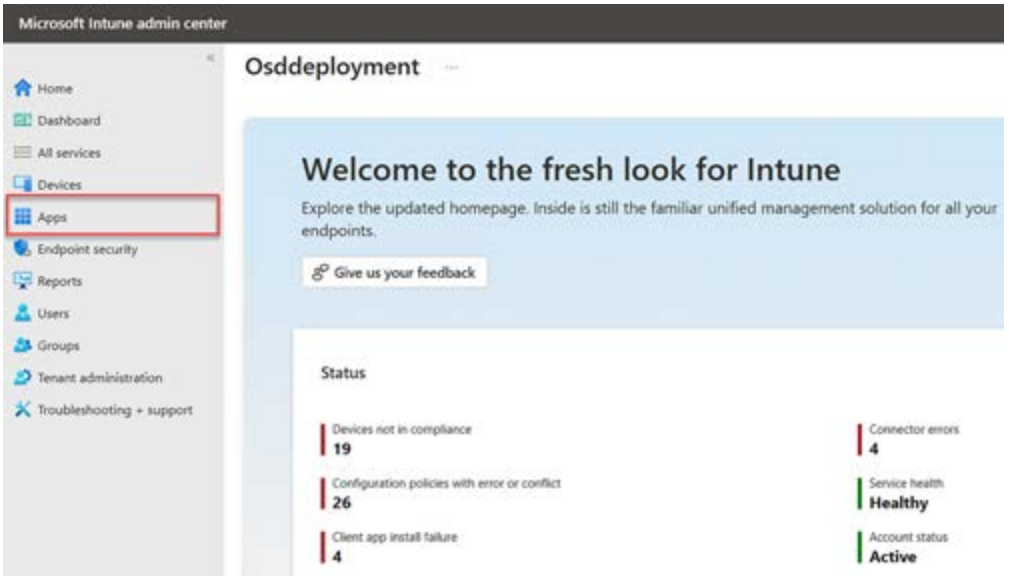


Figure 8.14: Apps

9. Click on **Windows**:

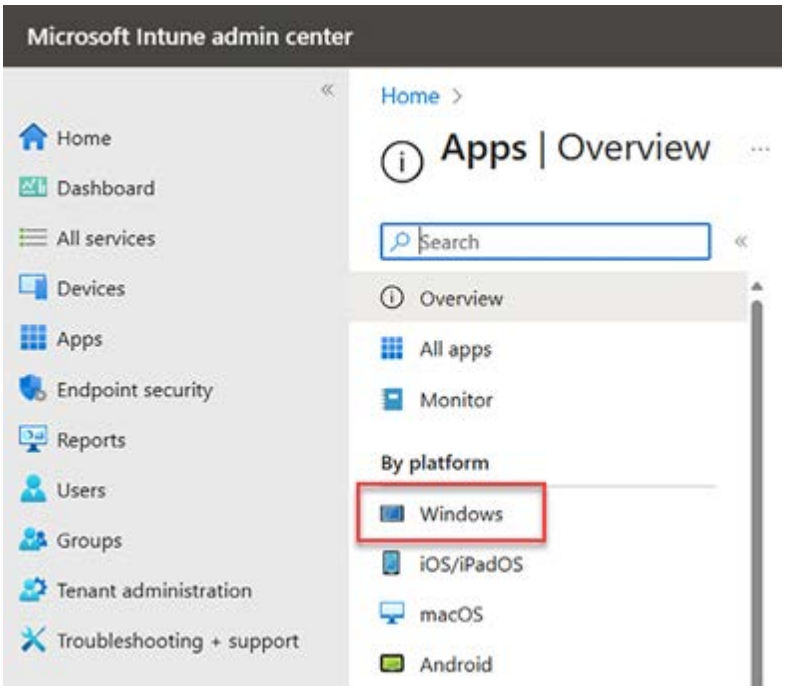


Figure 8.15: Apps | Windows

10. Click on **+ Add:**

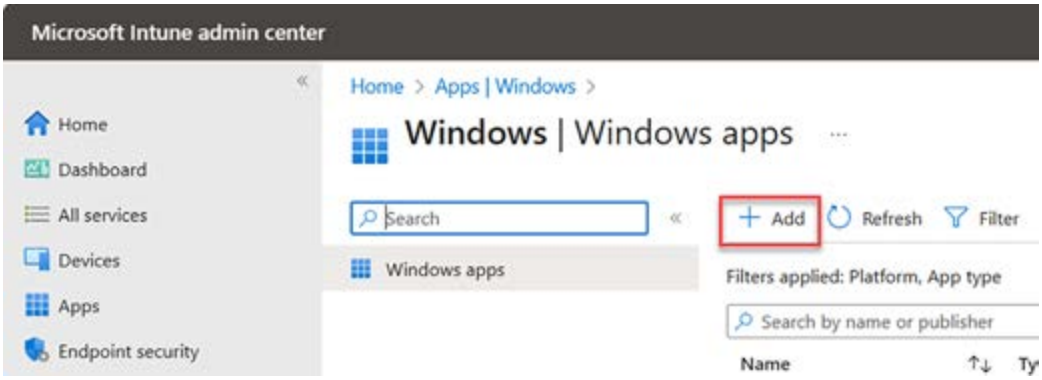


Figure 8.16: Adding an app

11. Select **Windows apps (Win32)**. Click on **Select app package file:**

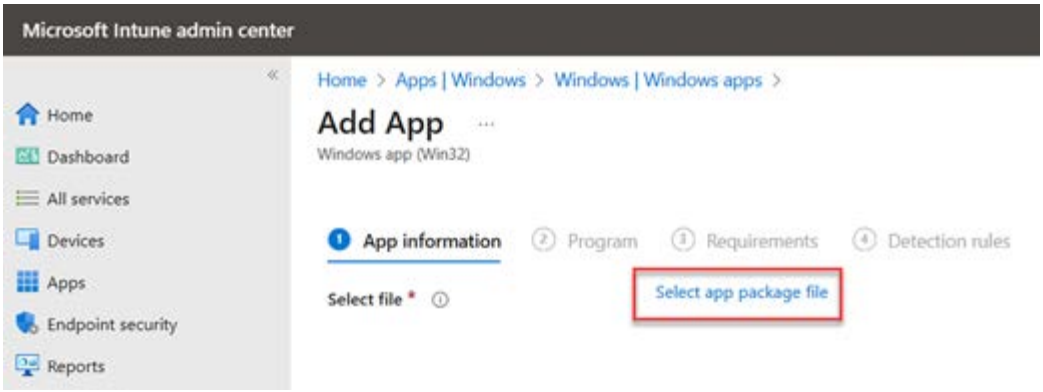


Figure 8.17: Select app package file

12. Browse and select the **.intunewin** package file created earlier. Click on **OK:**

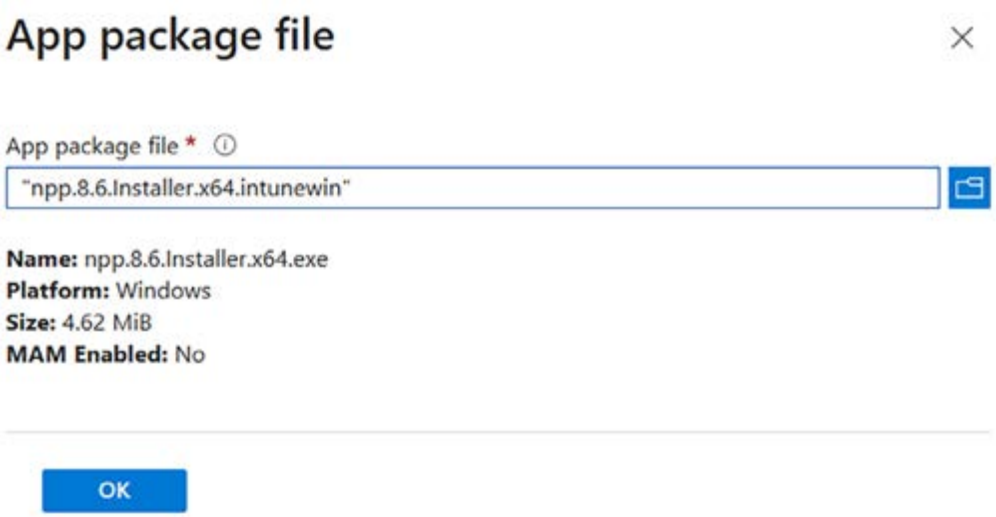


Figure 8.18: App package file

13. On the next screen, you can customize the name of the app.

    Optional: Set **Show this as a featured app in the Company Portal** to **Yes** if you prefer to make enrollment optional as regards user installation:

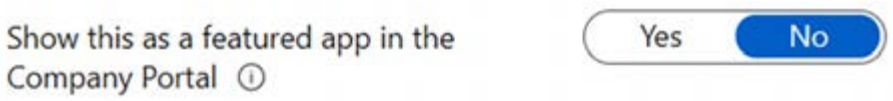


Figure 8.19: Showing as a featured app

14. Enter the settings in the **App information** tab as follows:

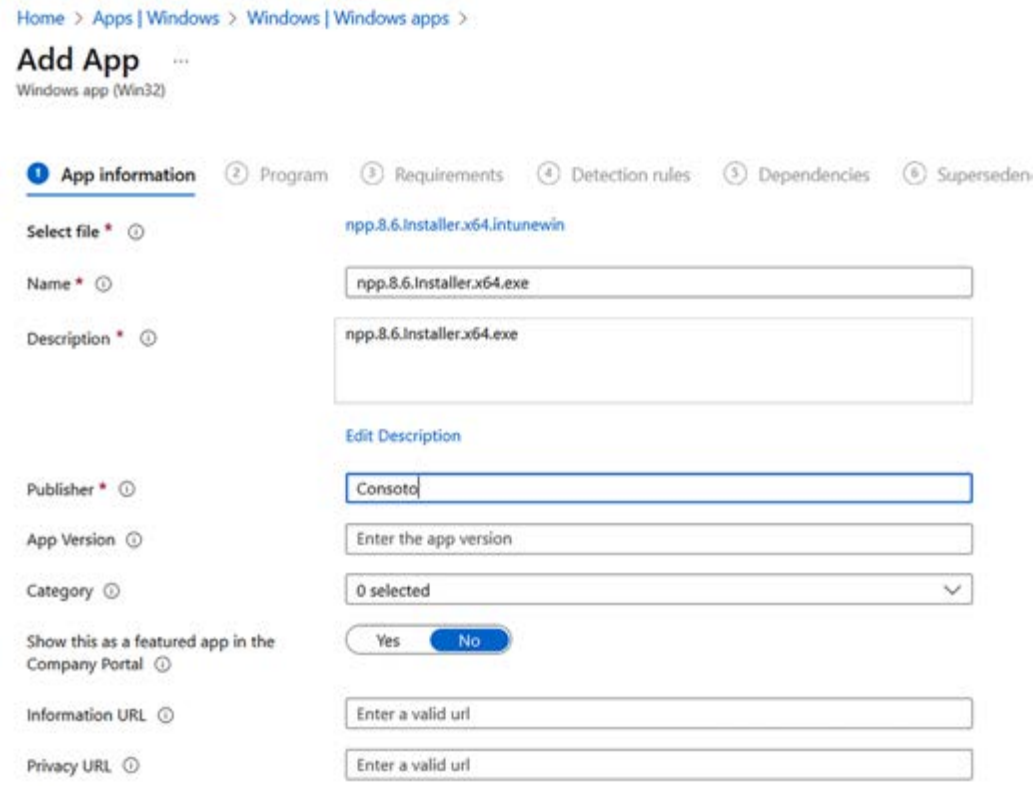


Figure 8.20: App information

15. Make sure to enter the app version manually to use features such as supersedence better, as this allows you to detect previous versions more easily when the application vendor doesn't include the version in the installation file:



Figure 8.21: App Version

16. Enter the application-specific parameters to provide the silent installation of your application: `npp.8.6.Installer.x64.exe /S`.

    Pick the installation behavior of your application. If it's a system install application (machine context), select **System** (the most common choice), or select **User** if the app should be installed in user context:



Figure 8.22: Install behavior

17. If your app requires a reboot, please update the **Device restart behavior** section to whatever best fits your use case:

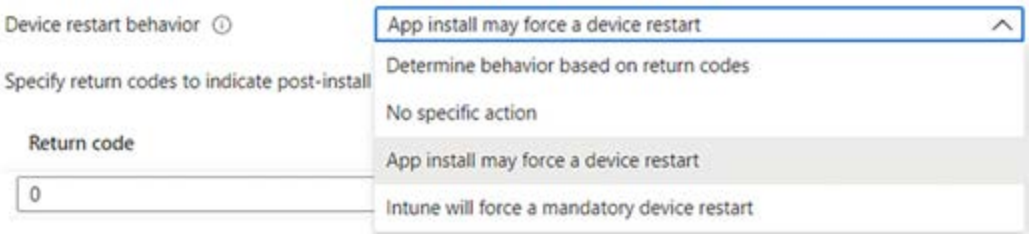


Figure 8.23: Device restart behavior

18. Provide the minimum app requirements, for example, the OS version.

    Use the return codes to address the issue of whether the app has been installed successfully. This allows you to detect any failures in other Microsoft Intune services, such as Endpoint Analytics, so as to perform auto-remediation actions:



Figure 8.24: Return codes

19. Once all the settings are entered, click on **Next** to define the requirements of the application:

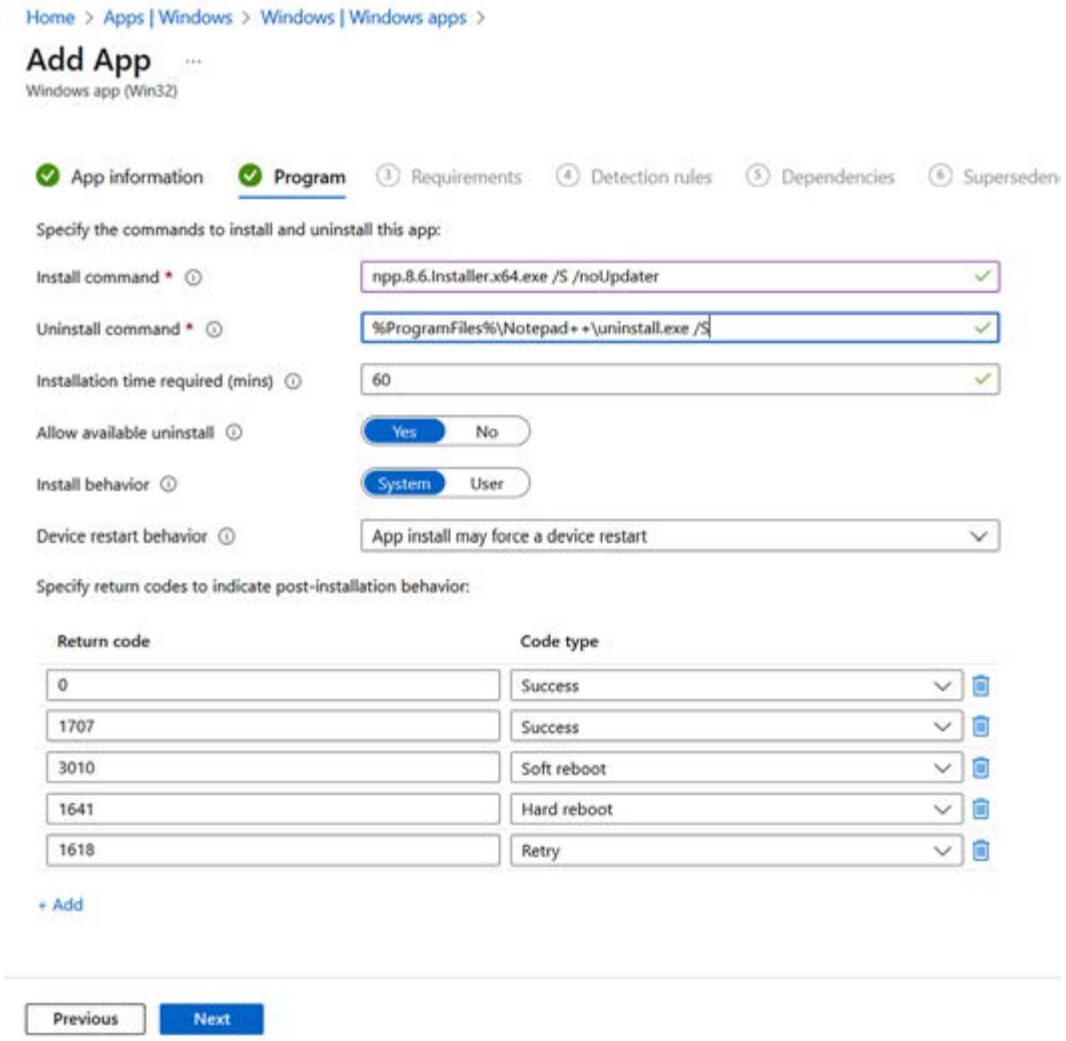


Figure 8.25: Add App | Program

20. **Allow available uninstall** gives the end user the option to uninstall the app from the Company Portal.



Figure 8.26: Allow available uninstall

21. Specify the requirements that devices must meet before the app is installed. The following requirements are supported, as you can see:

    - **Disk space required (MB)**
    - **Physical memory required (MB)**
    - **Minimum number of logical processors required**
    - **Minimum CPU speed required (MHz)**
    - **Configure additional requirement rules**

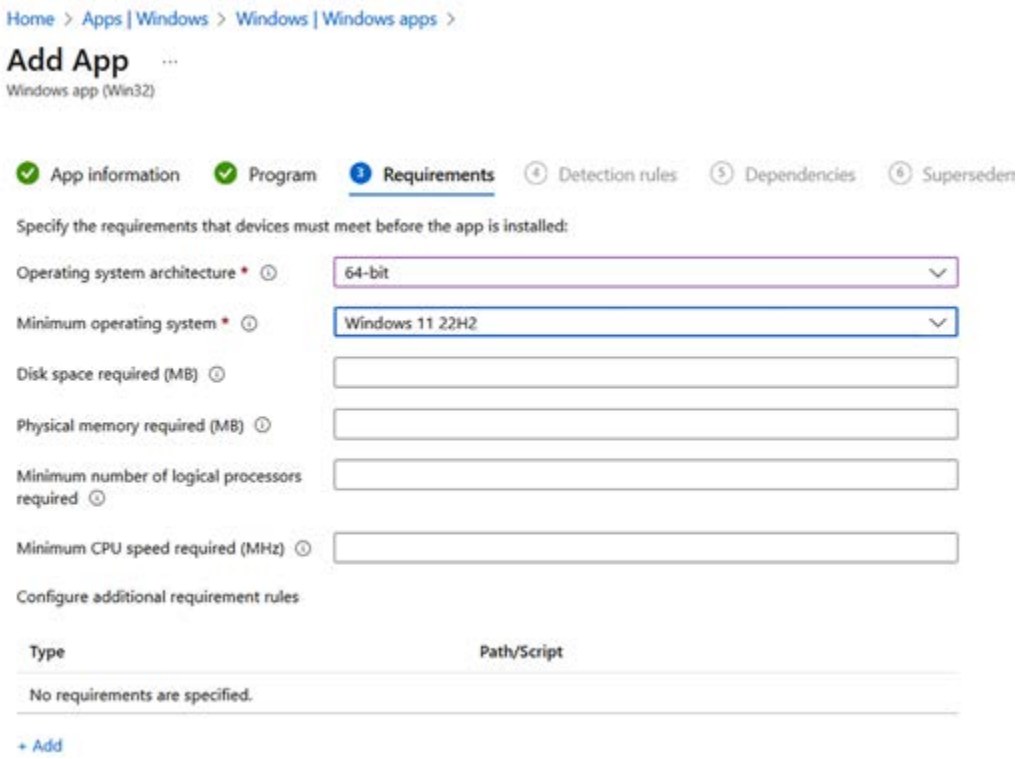


Figure 8.27: App requirements

22. As explained at the start, you could also add scripted actions to the installation of your application as a requirement. For example, you can run a PowerShell script first:

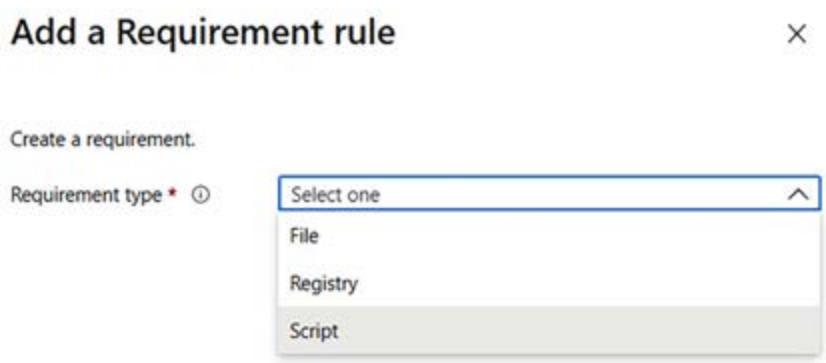


Figure 8.28: Add a Requirement rule script

23. You must add the information of the script and the requirements when you want to use this feature or run this script before the installation process:

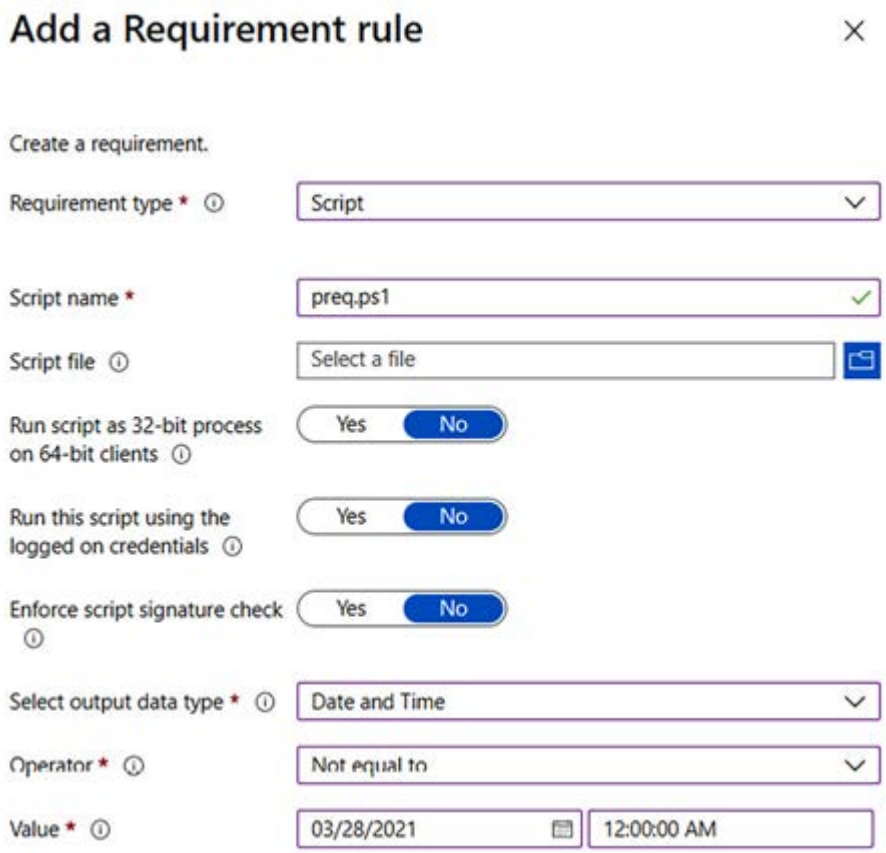


Figure 8.29: Add a Requirement rule

24. Create the detection rule to check whether the application has been installed as it indicates the presence of the app in the location you define:

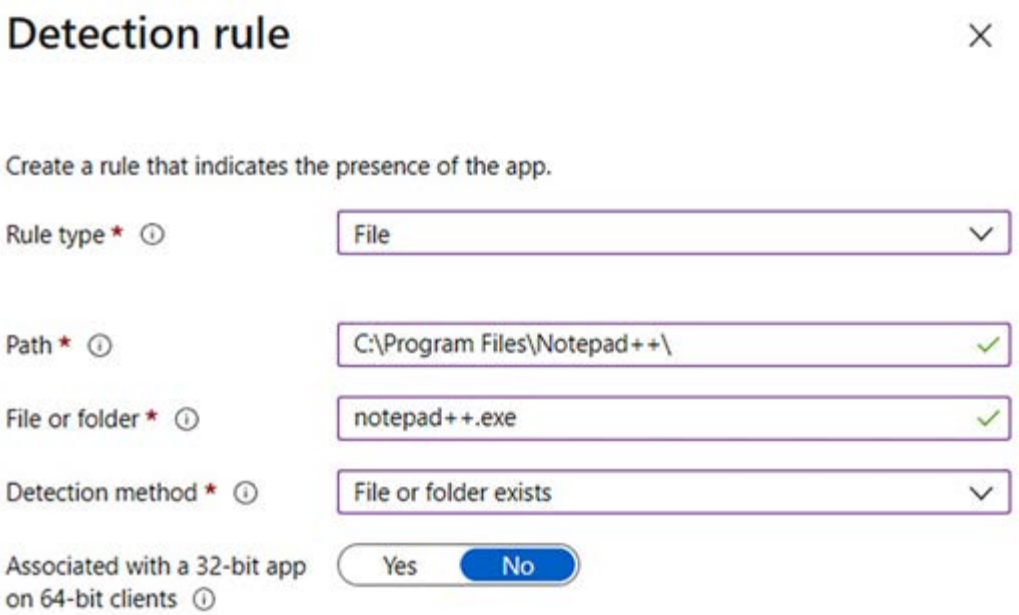


Figure 8.30: Detection rule

25. Software dependencies are applications that must be installed before the application (in this case, NotePad++) can be installed. To automatically install a child dependency app before installing the current parent app, enable the **Automatically Install** option. To only install the current parent app if the child dependency app is already detected on the device, disable the **Automatically Install** option. There is a maximum of 100 child dependency apps, including references to other apps outside of this view, forming a graph of apps. The total size of the dependency app graph is limited to a maximum of 100 plus the parent app (101 total).

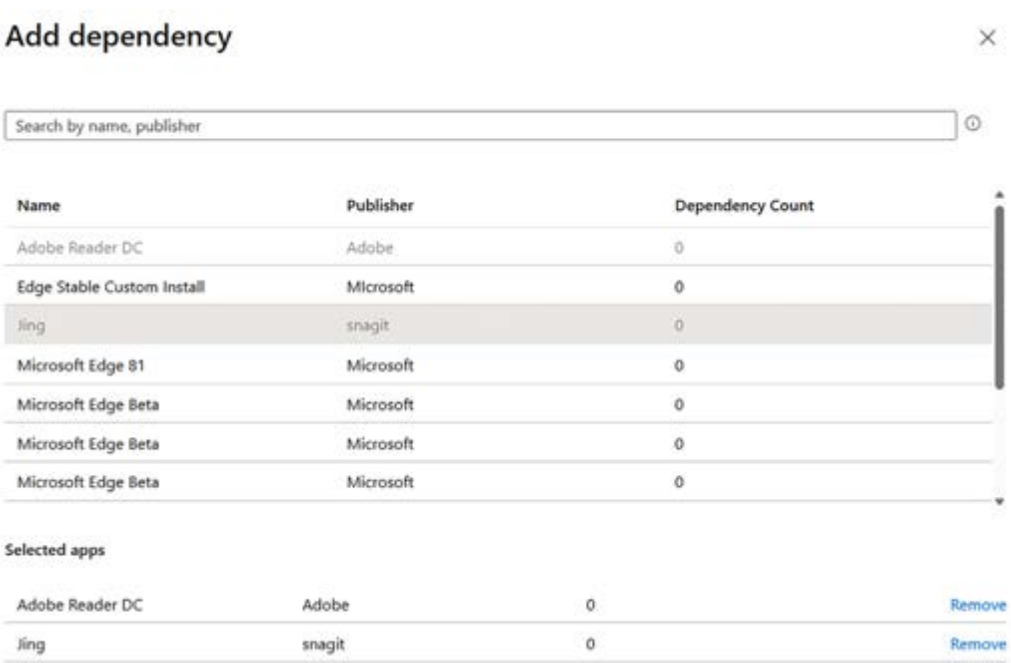


Figure 8.31: Add dependency

When adding dependencies to a Win32 app, you can browse between your already created Win32 apps or Microsoft Edge apps that are built in.



Figure 8.32: Add dependency

You need to select if you want to install apps with dependencies automatically.

Supersedence mode

In general, supersedence is where you update or replace something. In Intune, supersedence enables you to update and replace existing Win32 apps with newer versions of the same app or an entirely different Win32 app. This will enable you to do comprehensive versioning.

When you supersede an application, you can specify which app will be updated or replaced. To update an app, disable the **Uninstall previous version** option. To replace the application version, you must enable the **Uninstall previous version** option. There is a maximum of 10 updated or replaced apps, including references to other apps:

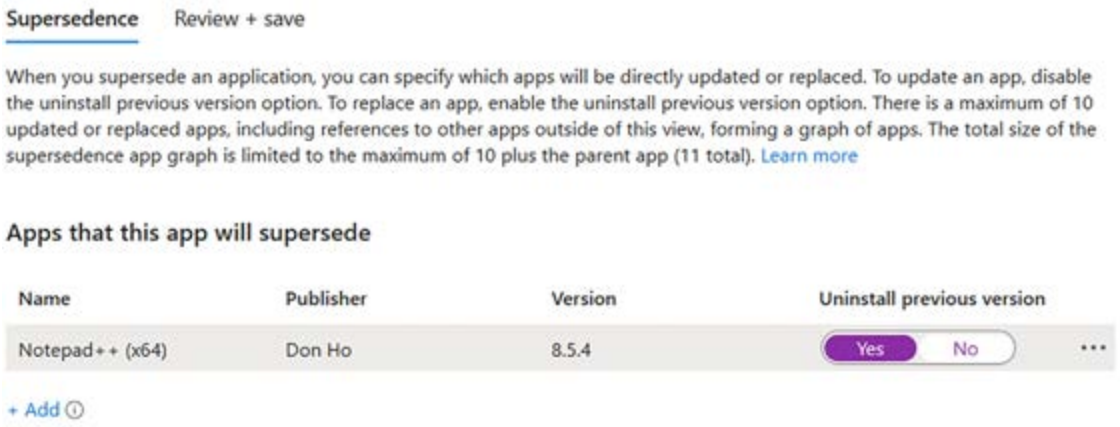


Figure 8.33: Supersedence



When using supersedence, make sure the application version is listed correctly as this makes it much easier for IT admins to detect previous versions.

1. Select the version of the application that you want to supersede/upgrade:



Figure 8.34: Add Apps supersedence

2. Assign the application to an Entra group or all devices, to enforce deployment to your Windows devices:

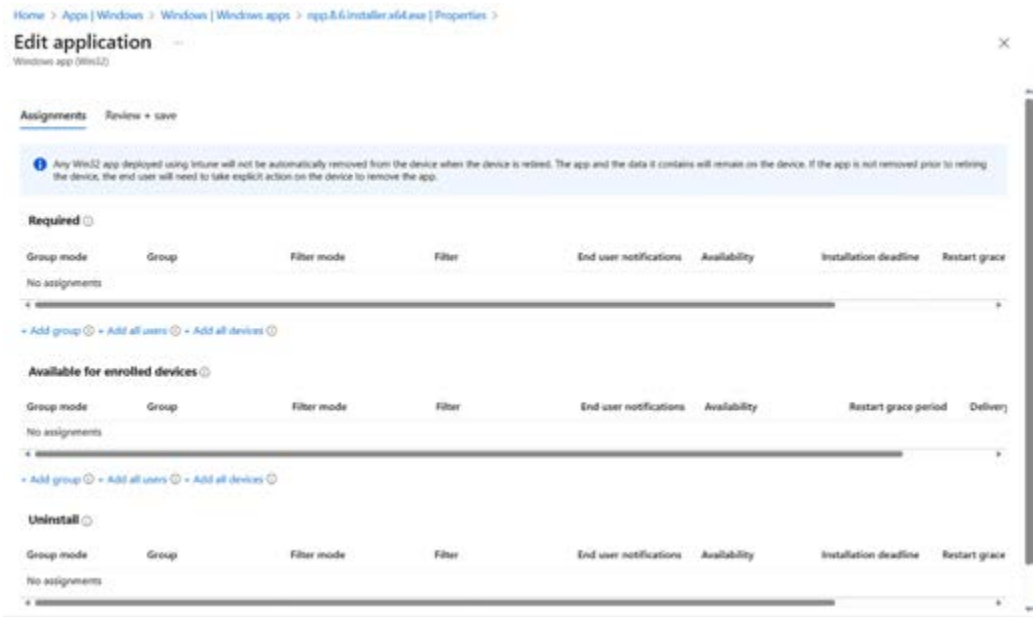


Figure 8.35: Add Apps – Assignments

3. Edit the assignment if you want to enforce the enrollment or update process.
4. Other great options include the option to schedule the update process based on different time zones and sequences that you can define:

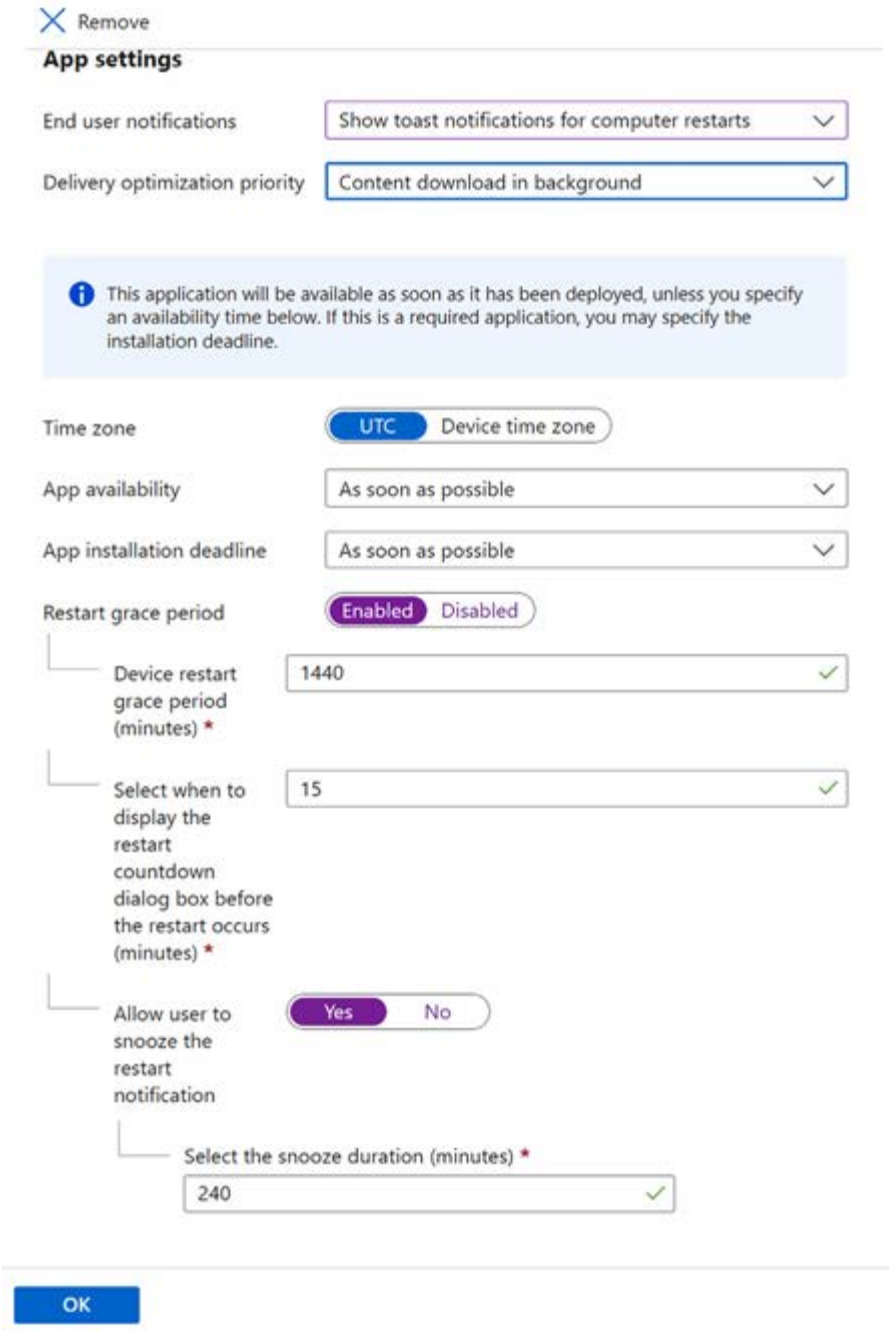


Figure 8.36: Assignment settings

5. You have the option to configure end user notifications to one of the following options:
    - **Show all toast notifications**
        - This will show all toast notifications, such as information about downloading, installation, and computer restart.
    - **Show toast notifications for computer restarts**
        - This will suppress all toast notifications except for computer restarts.
    - **Hide all toast notifications**
        - This will hide all toast notifications, including computer restarts. This is a great option for KIOSK devices, devices that have attached production equipment and have no users working directly on the device, and so on.
6. You have the option to configure app availability to:
    - As soon as possible, which will be at the next sync of the Intune Management Extension client on the Windows device.
    - A specific date and time and specify your date and time. The date and time specify when the app is downloaded to the user's device (not the installation time).
7. Set the app installation deadline to:
    - As soon as possible – so the app will start installing as soon as the content is downloaded to the device.
    - A specific date and time and select your date and time. This date and time specify when the app is installed on the targeted device. When more than one assignment is made for the same user or device, the app installation deadline time is picked based on the earliest time possible.
8. Restart the grace period to:
    - **Enabled**: When configured to enabled, you will get more configuration options in the UI.
    - **Disabled**: This means that the device can restart without any end user warning.
9. The restart grace period starts as soon as the app installation has finished on the device.
10. You can customize the following options:
    - **Device restart grace period (minutes)**: The default value is 1,440 minutes (24 hours). This value can be a maximum of 2 weeks.
    - **When to display the restart countdown dialog box before the restart occurs (minutes)**: The default value is 15 minutes.

- Allow a user to snooze the restart notification:
  - **Yes**

    Select the snooze duration (minutes): The default value is 240 minutes (4 hours). The snooze value can't be more than the reboot grace period.
  - **No**

11. Confirm that your app configuration is set. If everything aligns, you can start the deployment by clicking on **Create**. *Always double-check your settings*:

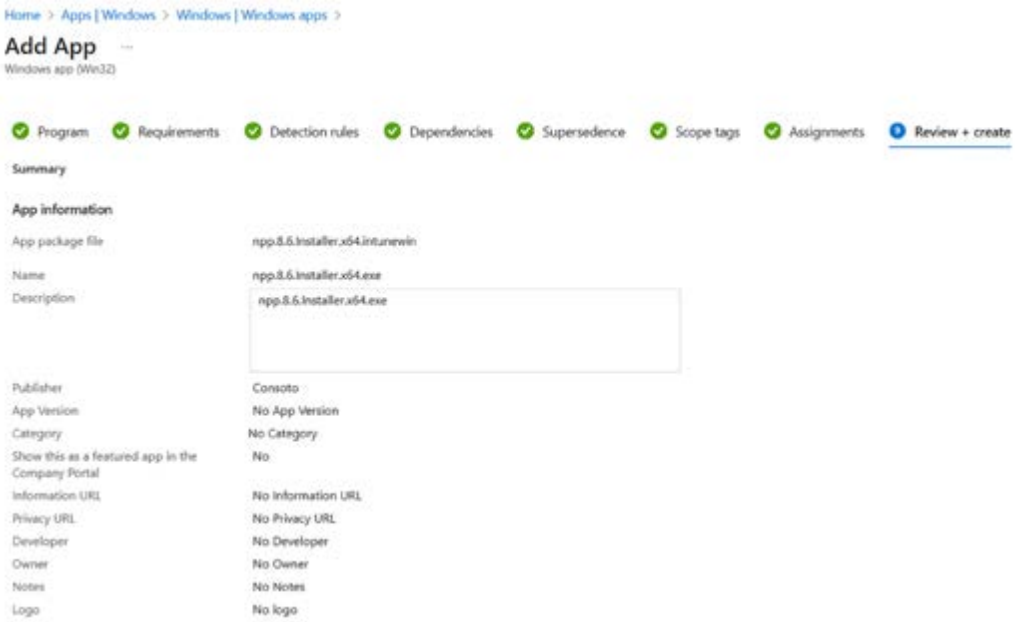


Figure 8.37: Review + create

12. The application will now be pushed to all the devices of users who are part of the Entra group:

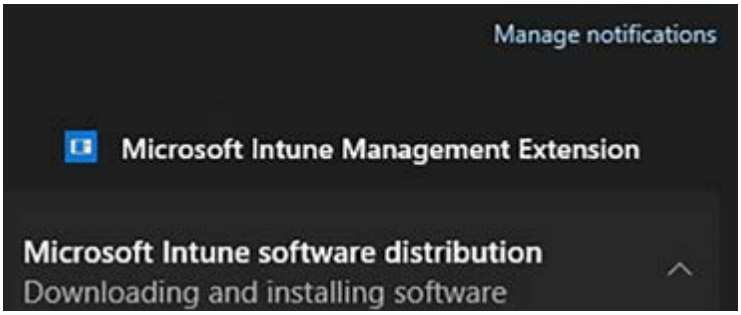


Figure 8.38: Microsoft Intune Management Extension toast notification

You can repeat the same steps for all your applications in your environment or choose to use MSIX for application virtualization first to simplify your application distribution process.

The application will show up as a recently added application in the user's **Start** menu.

Deploying Microsoft 365 apps

Office Click-to-Run is the new way of deploying Microsoft 365 apps – Office to your endpoints. The installation takes place in the following five different stages, as the following example describes, and involves active downloading from the internet. Therefore, the installation elements are very small.

Microsoft 365 apps are not like other apps in Microsoft Intune, as there is a policy that is deployed to the managed devices. The policy is similar to other CSPs deployed through the MDM channel to the device:

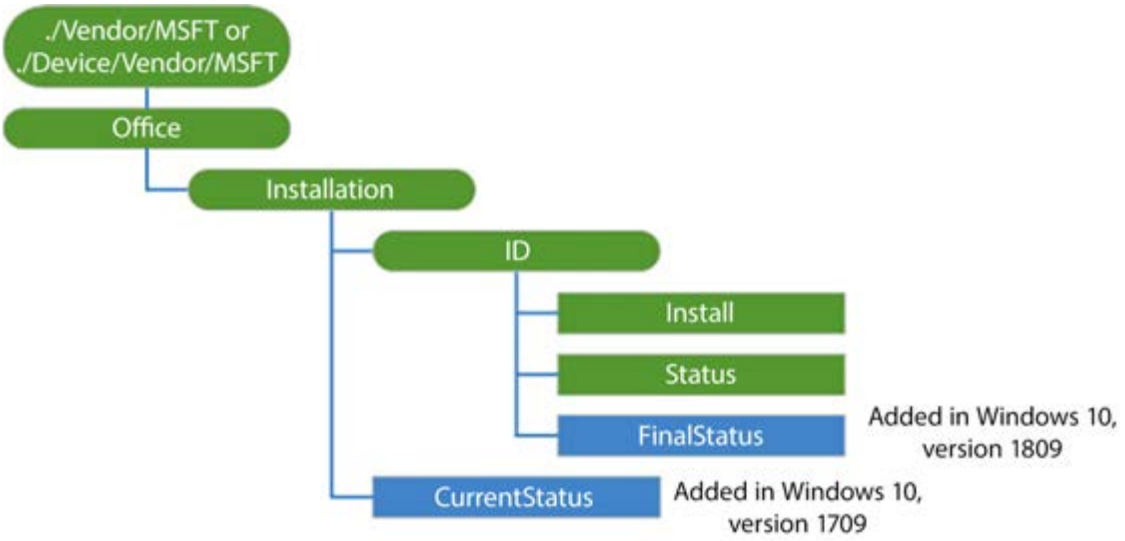


Figure 8.39: Office CSP

As it is a CSP policy and not a Win32 app, that is also the reason why you cannot use it as a dependency in a Win32 app. The CSP writes to the registry key `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OfficeCSP`, where it creates a default key with the value `http://go.microsoft.com/fwlink/?LinkID=829801`, at which point the `setup.exe` file downloads the file to the local device together with the XML file stored in the same registry location with a GUID.

The combination of `setup.exe/configure` (the name of the Microsoft 365 Apps XML file) will then start downloading all the binaries from the Office CDN (the default option in the Microsoft Intune UI and configuration XML).

Once installation is complete, the `FinalStatus` registry key will be updated as follows:

- When `status = 0: 70` (succeeded)
- When `status != 0: 60` (failed)

Microsoft Intune app delivery supports the direct enrollment of Microsoft 365 apps from within the app profile configuration menu.

It's just a drop-down menu that allows you to include or exclude Microsoft 365 apps from installation (without the need for an ODT – XML file):

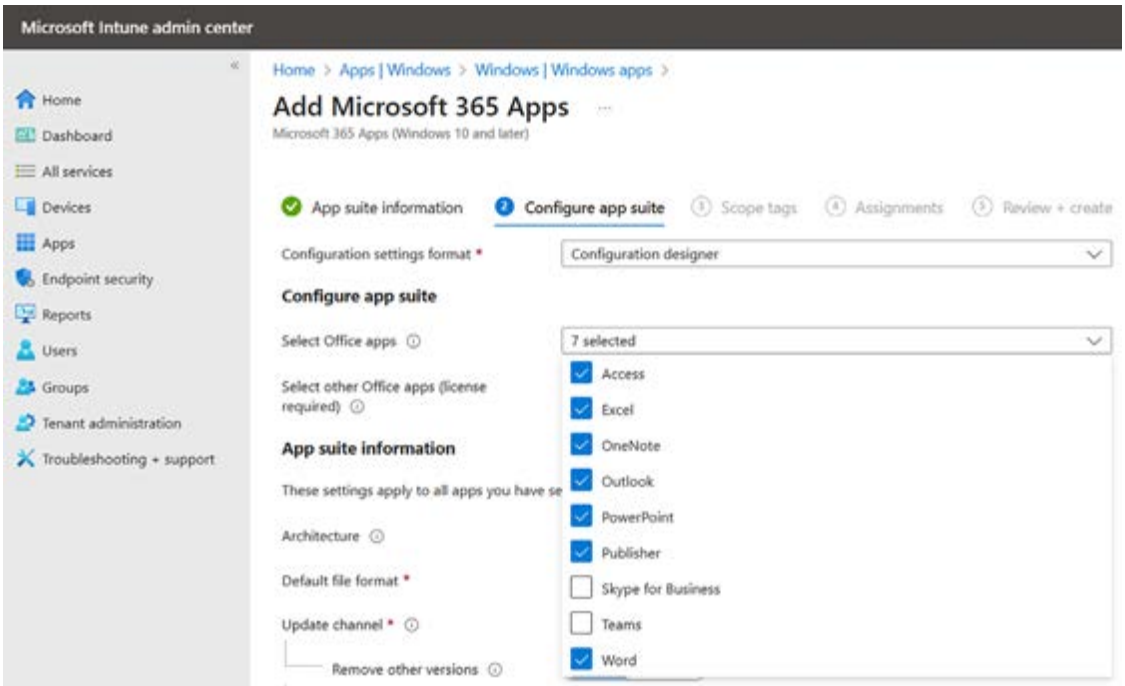


Figure 8.40: Add Microsoft 365 Apps

When you have selected the Office apps you want in this deployment, you can continue in the Microsoft 365 Apps wizard.

Update channels

Select whether to use the 32- or 64-bit version of your chosen Microsoft 365 apps; the Microsoft recommended option is 64-bit.

Set the default file format: **Office Open Document Format**

Select the update channel that best aligns with your business requirements; we have seen a huge uptake in customers running Monthly Enterprise Channel after the introduction of Microsoft 365 Copilot.

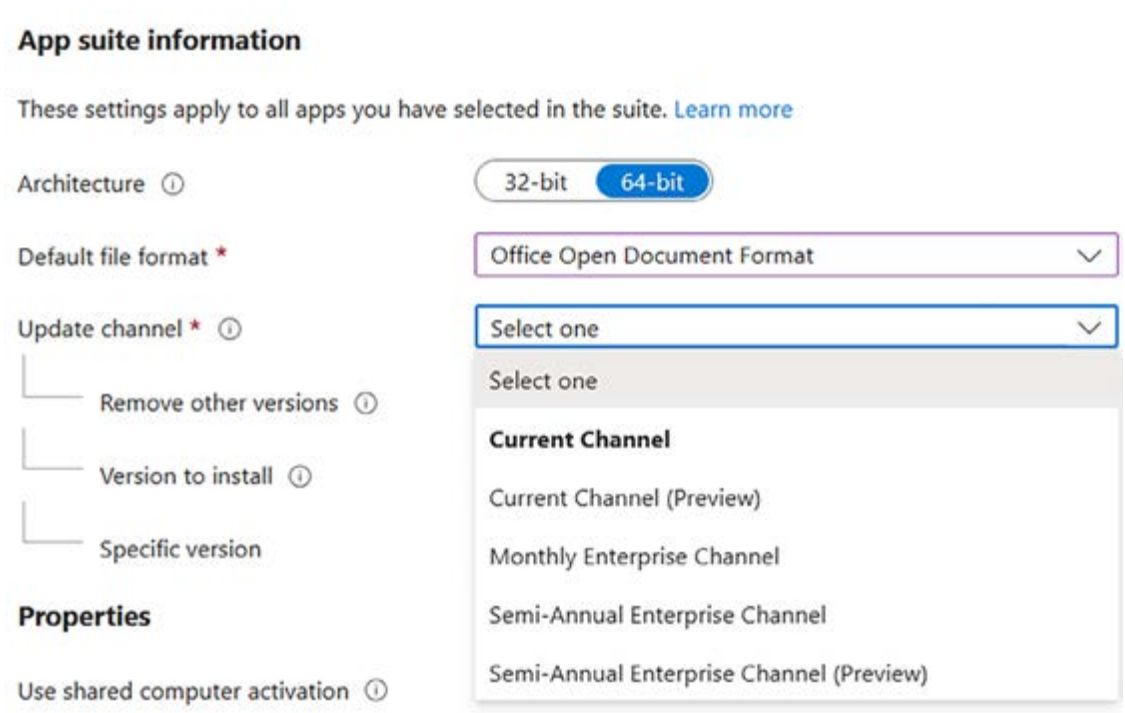


Figure 8.41: App suite information

Other great settings that are directly supported from within the console are the following list of features:

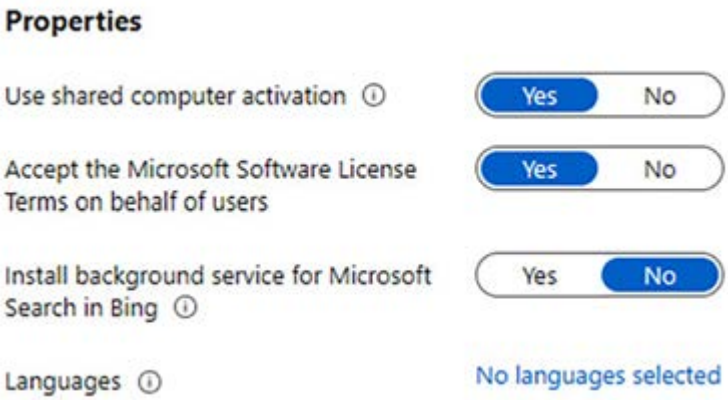


Figure 8.42: Properties

Shared computer activation lets you deploy Microsoft 365 apps to computers that are used by multiple users. Normally, users can only install and activate Microsoft 365 apps on a limited number of devices, such as five PCs. Using Microsoft 365 apps with shared computer activation doesn't count against that limit.

Office Customization Tool

The Microsoft 365 app type enrolment flow also supports custom configuration XML files. The Office Customization Tool is normally used in on-premises environments to deploy Office in large organizations.

You could incorporate that configuration set inside your app type configuration and Intune will take over the specific exclusion and other configuration settings. If you, for some reason, need to install Office LTSC Pro 2021 with Intune:

1. You can start with the Microsoft 365 Apps Admin Center (`https://config.office.com`).
2. Walk through the wizard and you will get a `.xml` file as output that you can download and use in Intune.

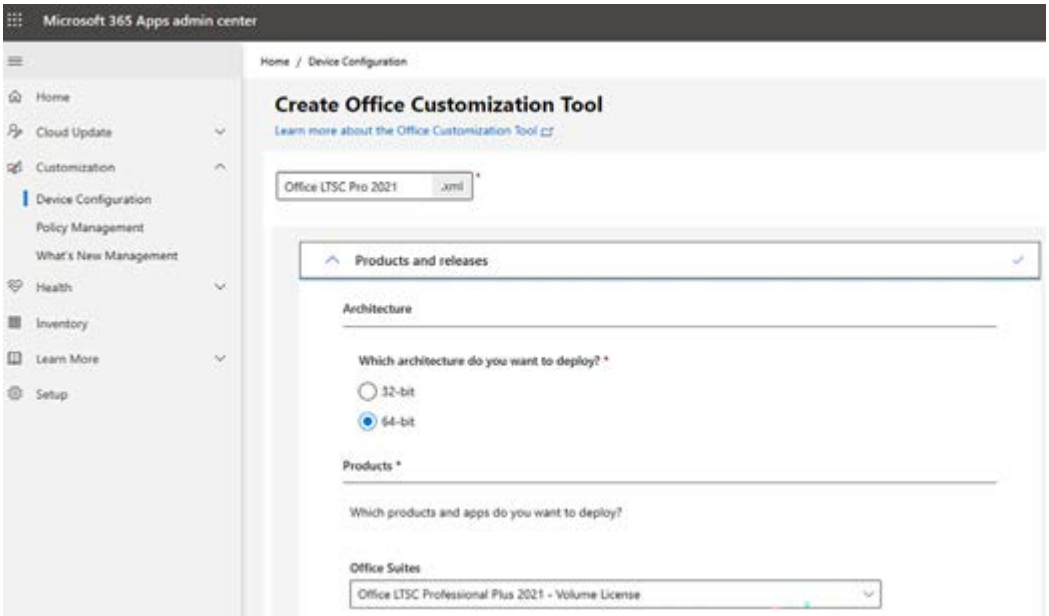


Figure 8.43: Office Customization Tool

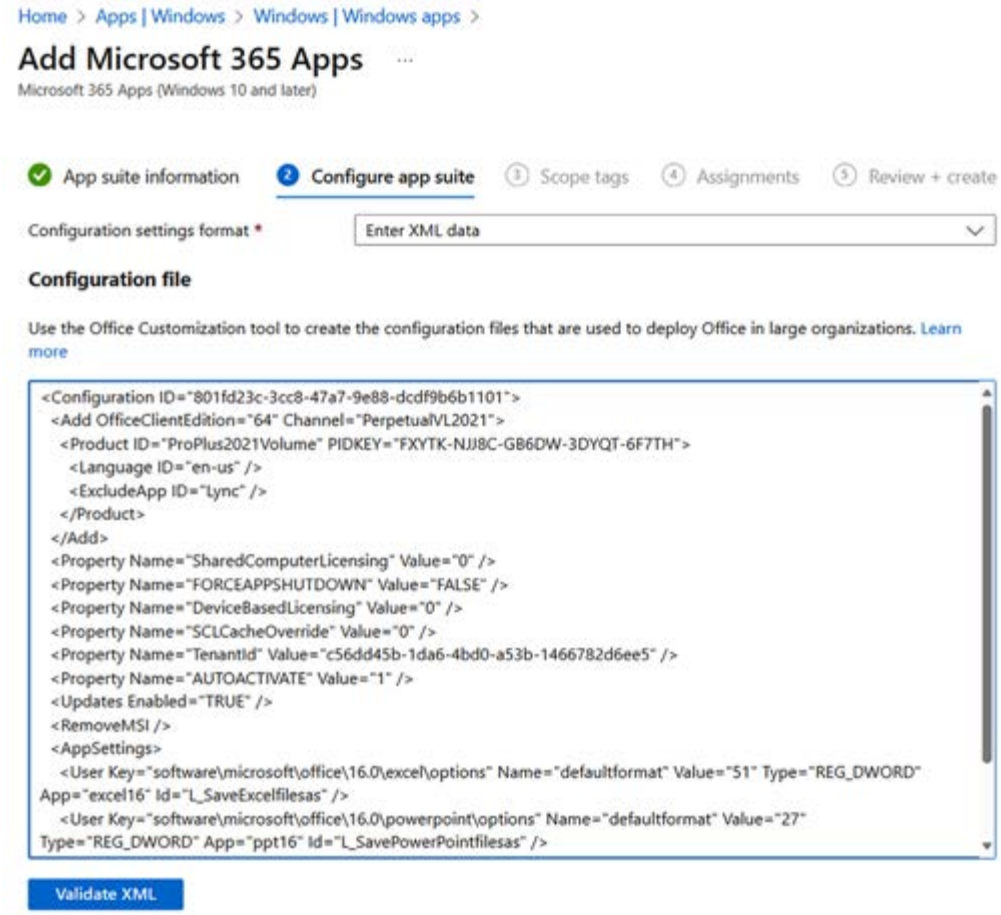


Figure 8.44: Configuration file

3. Choose the Office language versions that you want to install. Office automatically installs versions for any languages that have been installed in Windows. Use these settings if you want to install additional languages:

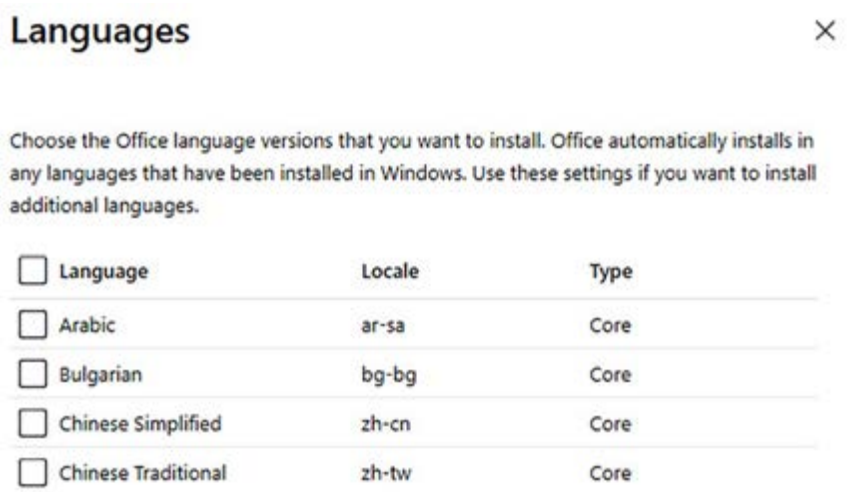


Figure 8.45: Languages

The Office language version needs to be the same as in the Microsoft 365 app that you are deploying to your users.

The reason for that and why you cannot create an additional Microsoft 365 app is that Office CSP only supports one assignment per device; this means if you assign multiple Microsoft Enterprise apps to your users' devices, you will not be able to get the correct reporting in the Company Portal on the devices.

Microsoft 365 Apps admin center

In *Chapter 6*, *Windows Deployment and Management*, we already talked a bit about updating Microsoft 365 apps in general. We're now going to talk in a little more detail about the following option inside the `https://config.office.com` admin center portal, which brings you to the following page:



The Microsoft 365 Apps admin center should be used in addition to the previous section regarding the delivery of Microsoft 365 apps.

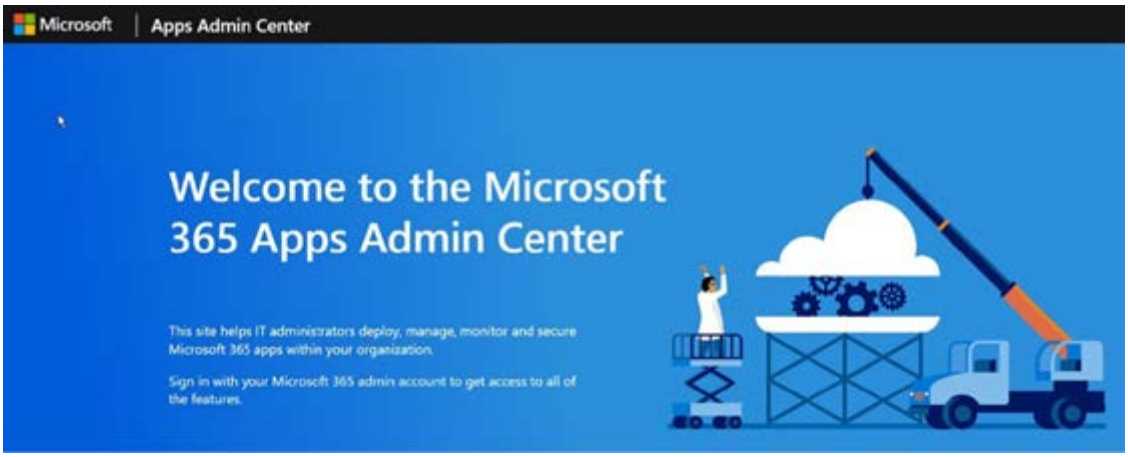


Figure 8.46: Microsoft 365 Apps admin center

After logging on with your (Intune) administrator credentials, you must go to **Servicing** to start creating custom profiles for Microsoft 365 apps.

Accept the terms to continue to the service to start provisioning and maintaining Microsoft 365 apps. *This process can take up to 10 minutes*:

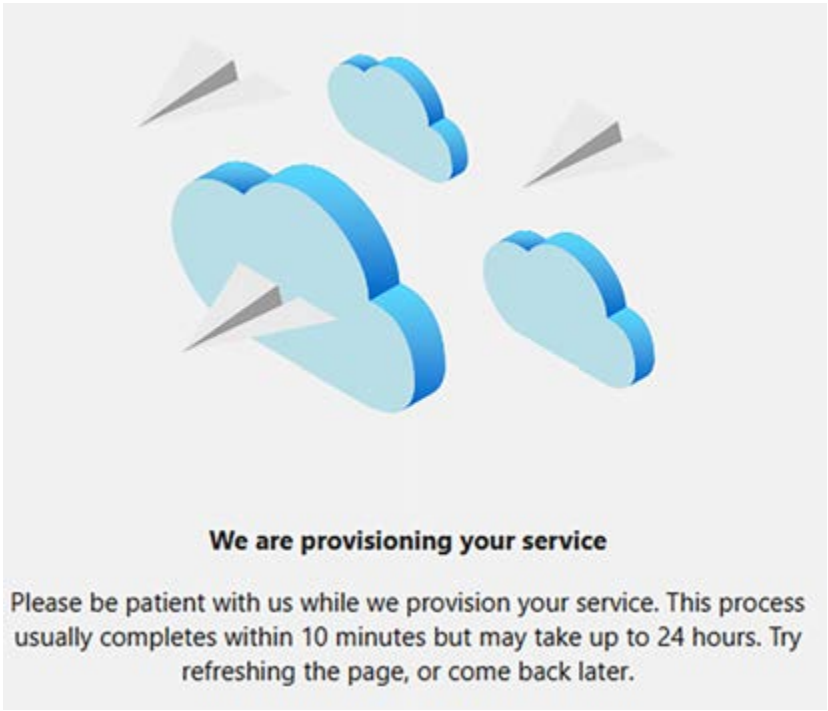


Figure 8.47: Provisioning your service

Once provisioning is complete, the following dashboard screen appears. Here's where we should start creating one of the two profiles for automatically updating and configuring Microsoft 365 apps:

- **Office policies:** Cloud-based policy management for Microsoft 365 allows you to manage policies for your organization.
- **Device Configuration:** Create configuration files that are used to deploy Office in large organizations with the Office Deployment Tool

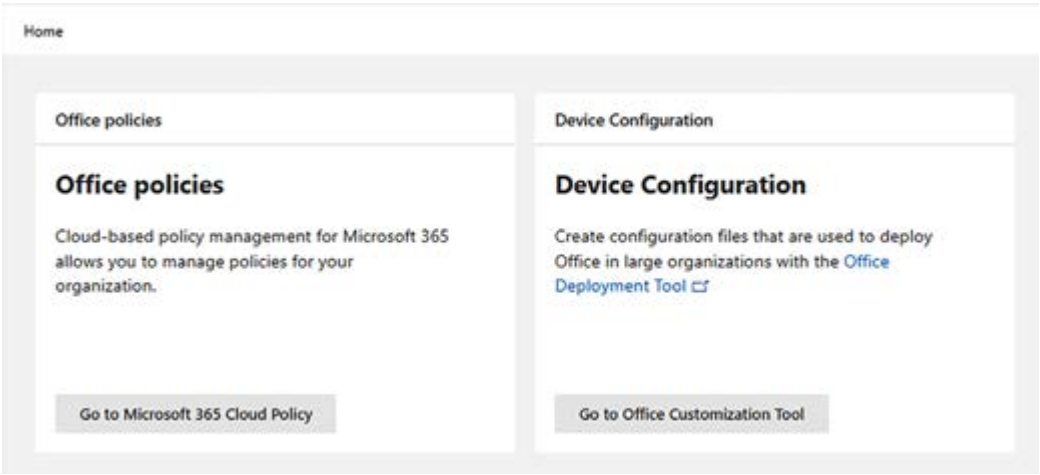


Figure 8.48: Home dashboard

Scroll down the page and click on the **Get started** button to (yes, you know the drill) get started:

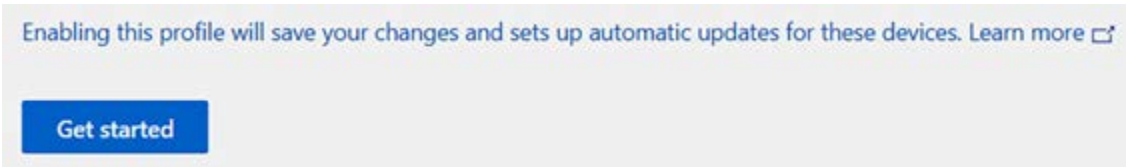


Figure 8.49: Get started

Getting started

The following wizard will guide you through creating the servicing profile.

The servicing profile automates the monthly updates for Office apps while providing you with control. Apps will be updated from the Office CDN and be placed on the Monthly Enterprise Channel. The setup wizard will walk you through the process of selecting devices that you would like to add to the profile along with other settings.

You can also set up other features, such as client-side update deadlines and update exclusion dates. You can revisit these options once the profile has been created through the **Settings** tab:

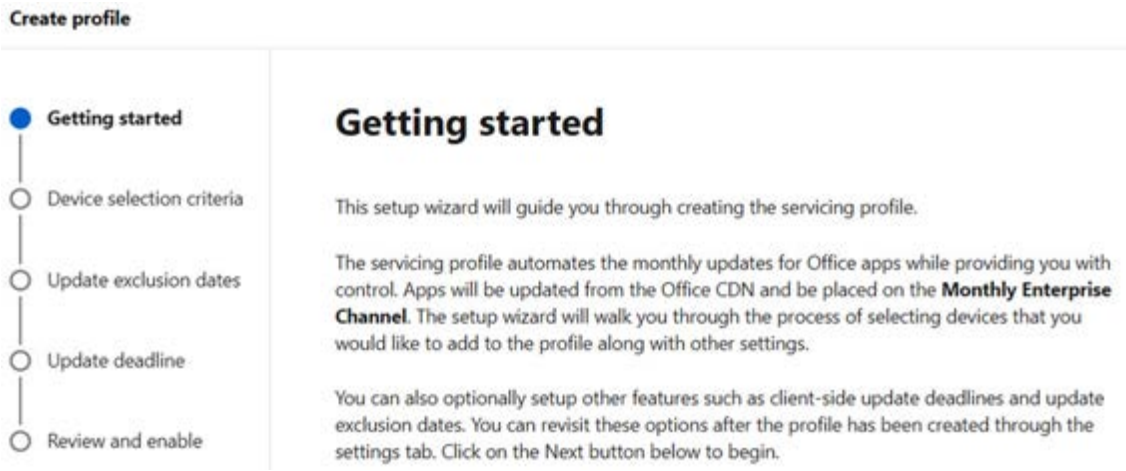


Figure 8.50: Getting started

Click on the **Next** button to begin.

Device selection criteria

You can configure your set of endpoints by adding additional criteria through the following filters.

Channels

In the **Channels** section, you define what devices will be moved from their current update channel to the Monthly Enterprise Channel.

For security purposes, you could exclude add-ins and macro usage.

Current Channel will be the default selection when you sign in to the Microsoft 365 admin center. To change this, you must go to **Settings | Org settings | Services** and **Office installation options**.

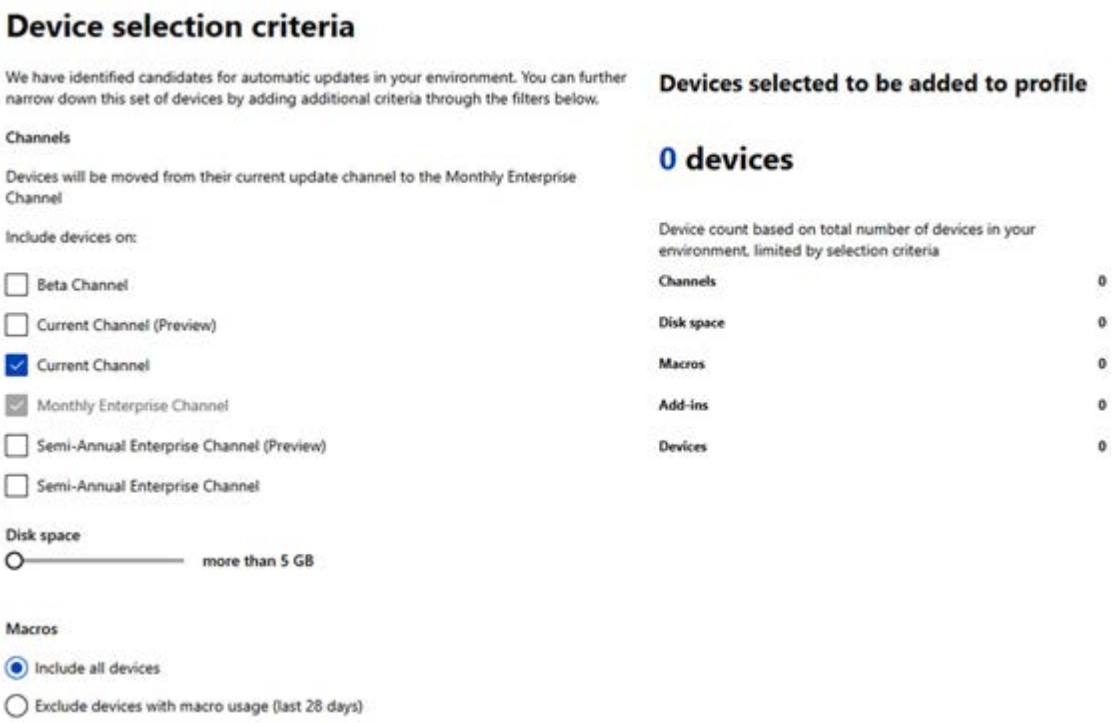


Figure 8.51: Device selection criteria

When you have selected the update channel, you can proceed to set up the update exclusion dates, as covered in the next section.

Update exclusion dates

Update exclusions can be used to prevent devices from downloading security and feature updates during specific moments. You can create different sets of exclusions that allow you to reduce the changes in your environment during busy periods.

Click on **No exclusion dates** if you want to add them at a later date:

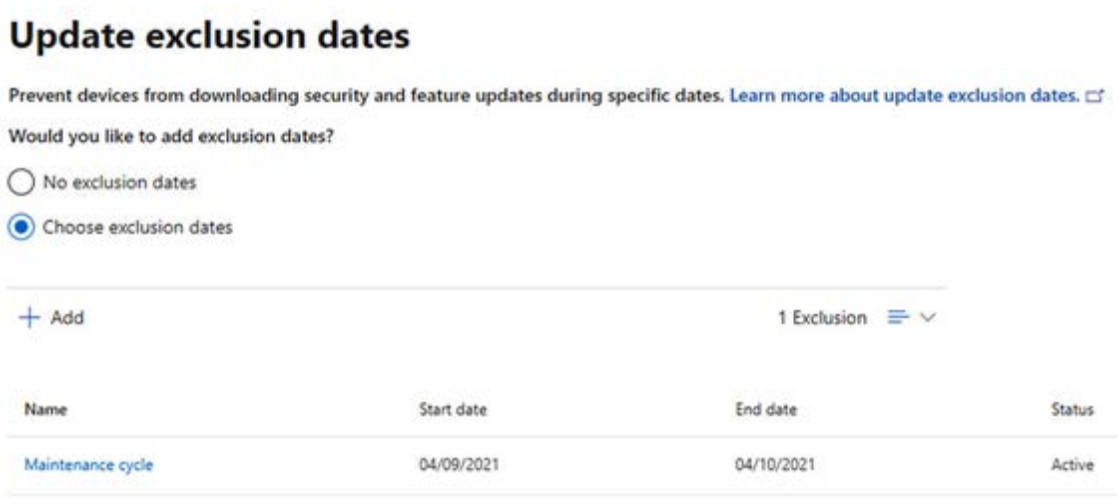


Figure 8.52 Update exclusion dates

When you have selected the update exclusion dates, you can proceed to update deadlines, which is covered in the next section.

Update deadline

Within the **Update deadline** menu, you can manage how updates are applied to Microsoft 365 apps for enterprise. This will help you to adjust the update cycle of your Office applications as well as offer capabilities to enforce updates or let users do it at their own pace.

There is also the option to give the user some spare days before the updates are enforced on the endpoint:

1. Click on **Next**.

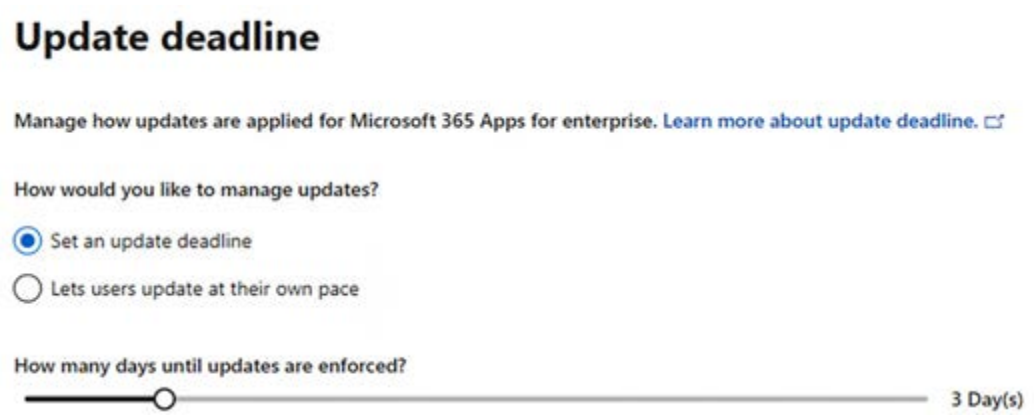


Figure 8.53: Update deadline

2. Review all your settings and click on **Create profile** to publish the settings to your devices:

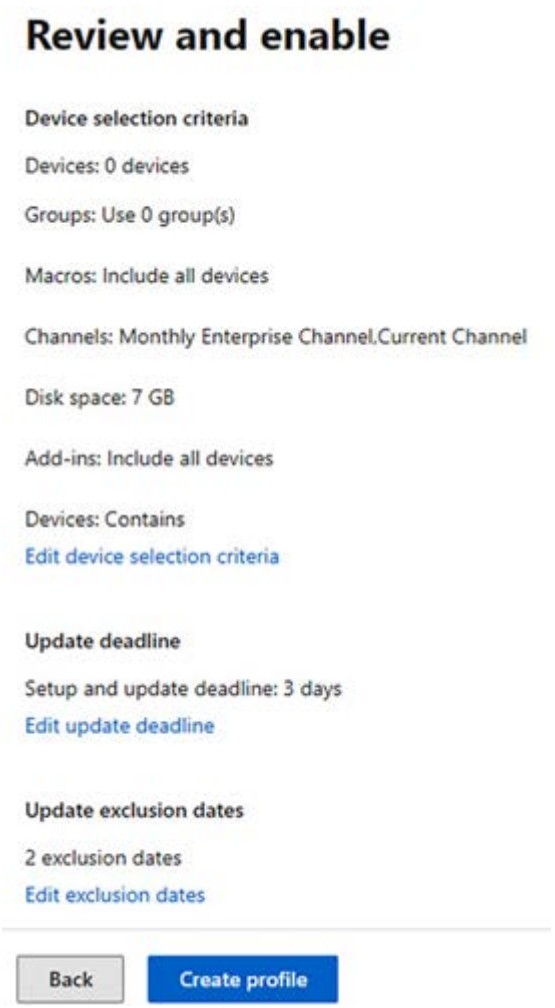


Figure 8.54: Review and enable

3. The profile has been created successfully:



Figure 8.55: Profile created

4. The **Servicing Profile** enrollment will now be created with the specifics you just defined in the profile.
5. You can modify the existing **Servicing Profile** easily by clicking on the settings in the following menu:



Figure 8.56: Monthly Enterprise Channel

This completes the configuration of Microsoft 365 apps updates. In the next section, we will cover Microsoft 365 app customization.

Microsoft 365 app customization

The other great feature within the **Apps admin center** portal is **Customization**. Here, you can provide default policy settings to your endpoints, all centrally managed:

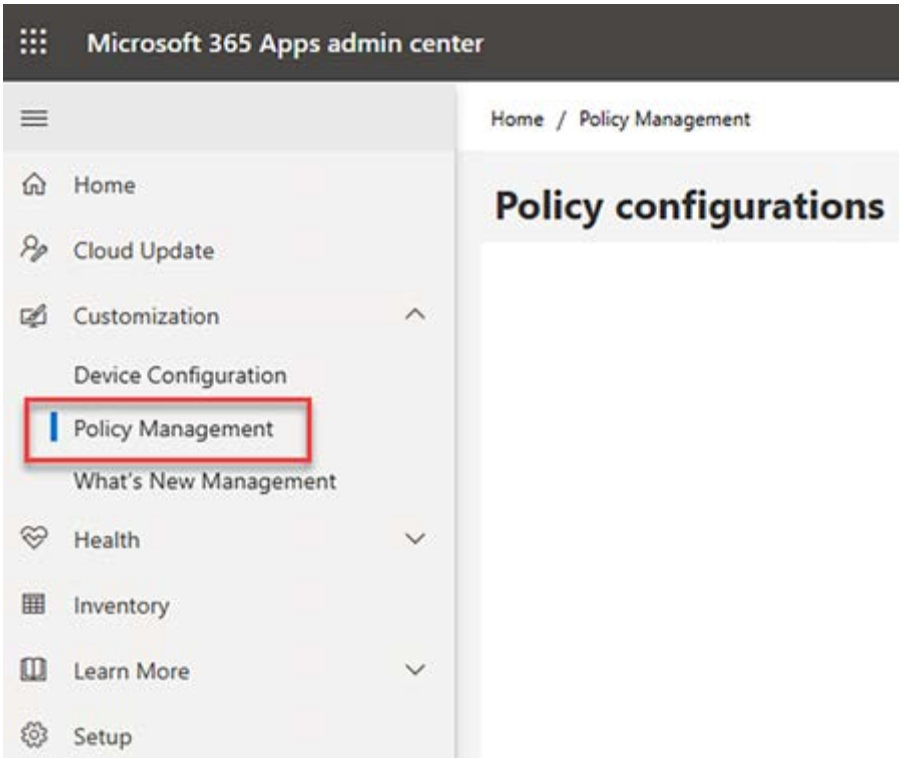


Figure 8.57: Policy Management

The **Create policy configuration** menu allows you to create different configuration sets within Office that you'd normally do as either an administrative template or via group policies for your legacy on-premises devices:

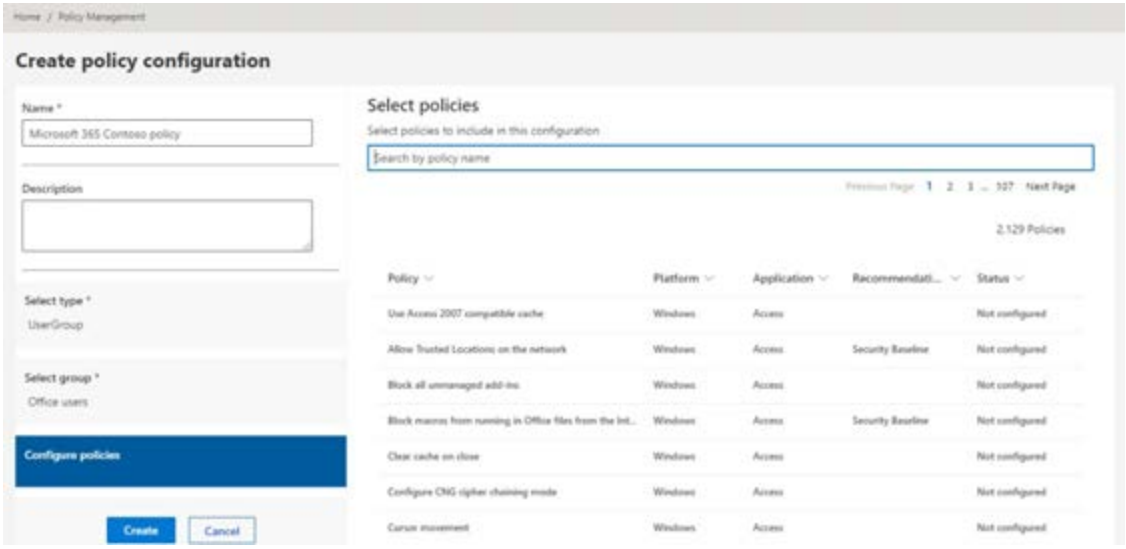


Figure 8.58: Create policy configuration

We'll go deeper into how you can leverage Microsoft Intune to set Microsoft 365 app policies in *Chapter 10, Advanced Policy Management*.

Deploying Microsoft Teams

MSIX packages are a container format for Windows applications that provide a modern packaging experience and simplify the deployment and updating of applications. Read more about the MSIX app format later in this chapter.

You can download an MSIX package for Microsoft Teams MSIX.

Microsoft provides an executable (`.exe`) file for the new Teams client so you can upgrade the application directly to the computers in your organization using your choice of software management tools, such as Intune or Configuration Manager.

The Teams installer installs the Teams MSIX package on a target computer, making sure that Teams can interoperate correctly with Office and other Microsoft software. As Intune natively supports MSIX, you can use the file directly instead of creating a Win32 app with `teamsbootstrapper.exe` that downloads and installs the Teams MSIX installer.

To download the MSIX package, you can follow these links:

Download Teams MSIX x64:

- `https://go.microsoft.com/fwlink/?linkid=2196060`
- `https://go.microsoft.com/fwlink/?linkid=2196106`

You can leverage Intune app deployment for LOB apps to deploy the new Teams client as an MSIX file.

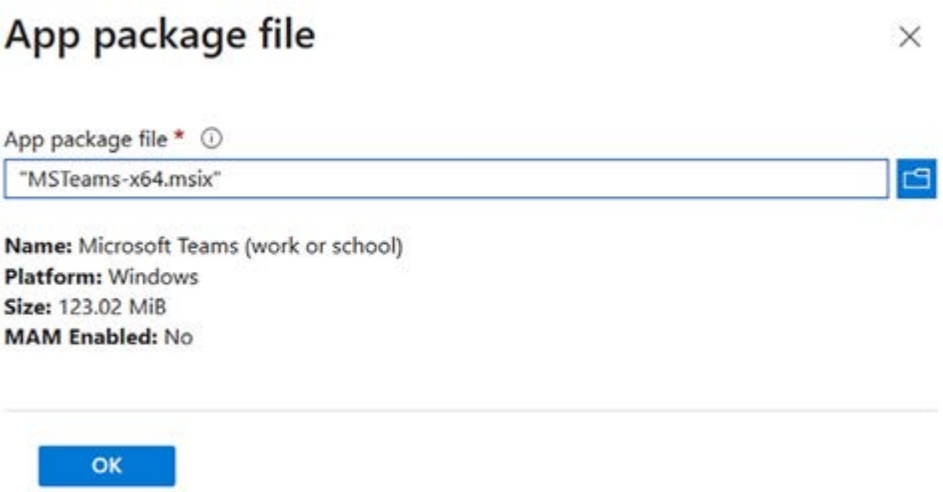


Figure 8.59: Teams MSIX Intune LOB app

Everything in the Intune Windows Universal line-of-business app is prefilled and just ready to deploy to either a user or a device group.

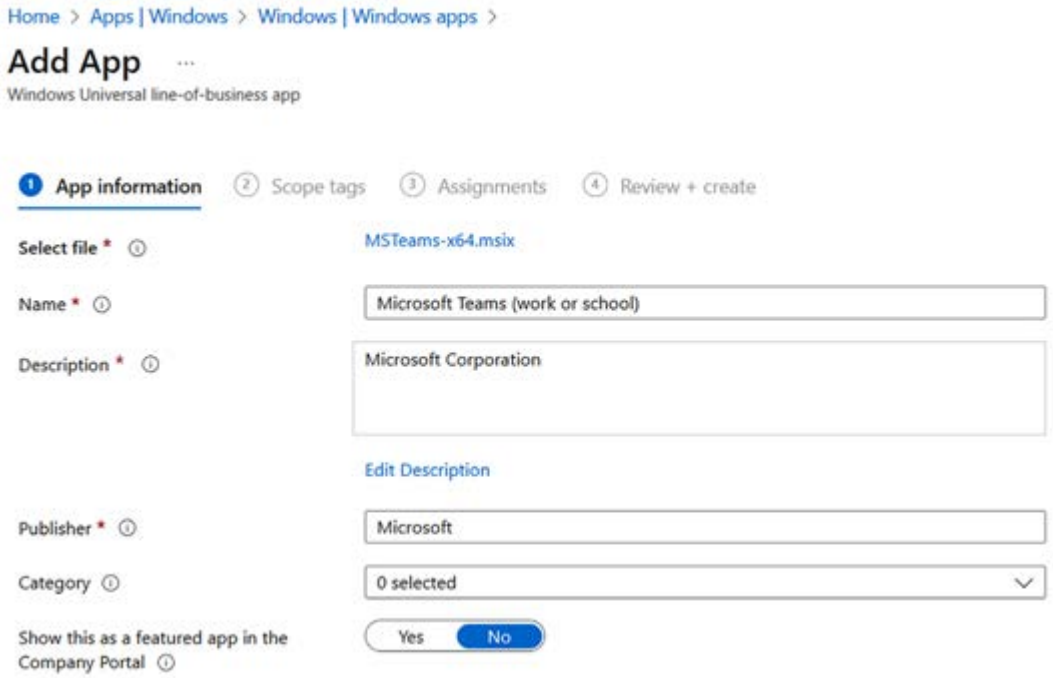


Figure 8.60: Add App



Microsoft Teams follows its own update process and does not follow the update process of other Microsoft 365 apps.

Teams client updates are not configured in your device management tools but in the Teams admin center. You can read more here: `https://learn.microsoft.com/en-us/microsoftteams/new-teams-deploy-using-policies?tabs=teams-admin-center`.

Deploying OneDrive

OneDrive isn't part of the Microsoft 365 app delivery process for the simple reason that OneDrive is mandatory for Windows Enterprise and is therefore included in the OS.

OneDrive automatically updates based on either the **Insiders**, **Standard**, or **Deferred** ring cycle. OneDrive checks for available updates every 24 hours when it's running as part of your endpoint.

The production ring (which is the default) receives updates every 20 days, whereas the deferred ring gives you a bit more flexibility as it updates every 2–3 months. During this timeframe, customers can deploy updates on their own, allowing them to record precisely when their software is updated. When the number of days is exceeded, the update will apply automatically:



Microsoft reserves the right to bypass the 60-day grace period for critical updates.



Figure 8.61: OneDrive update schedule

You can put your OneDrive client inside the **Deferred** ring via designated OneDrive policies, which we will explain in the next chapter.

When you want to force updates to your endpoint via Microsoft Intune, you could send the following command to your endpoints to make this possible. The `restart` parameter performs a reboot of your Windows Enterprise desktop:

```
Execute C:\<location>\OneDriveSetup.exe /update /restart
```

The OneDrive client is installed in each user's profile under `%localappdata%`. Beginning with the OneDrive sync client builds `19.174.0902.0013`, and later, you can install the OneDrive client on a per-machine basis. You only need to run `OneDriveSetup.exe/allusers` to convert the installation from per-user to per-machine:

This can be done by creating a PowerShell script and running it from Microsoft Intune to the device where you want the change:

```
####################################################
$url = "https://go.microsoft.com/fwlink/?linkid=2083517"
$output = "$ENV:temp"  + '\OneDriveSetup.exe'
$O4BPath = "$ENV:localappdata" + 'Microsoft/OneDrive/OneDriveSetup.exe'
#write $O4BPath
#write $output
IF(Test-Path $output)
{
}
ELSE {
Invoke-WebRequest -Uri $url -OutFile $output
   }
IF(!(Test-Path $O4BPath))
  {
    & "$output" + '/allusers'
  }
ELSE {teams
   }
```

This script will download the latest version of the OneDrive sync client and convert the installation to per machine in `Program Files (x86)\Microsoft OneDrive`.

Deploying Microsoft Edge

Microsoft Edge in the Beta or Dev channel has been fairly easy to distribute to your Windows devices ever since version 77: it completely integrates within Microsoft Intune, and this also applies to most of the policies that we'll cover in the next chapter.

In the **Intune apps** menu, you must add Microsoft Edge for Windows to install the Microsoft Edge browser on managed Windows 10 devices as **App type** to start the configuration:



Figure 8.62: Microsoft Edge for Windows 10

When you want to test new features earlier than the others that are active in the **Stable** ring, you can simply change the **Channel** setting to whatever best suits your use case.

You could also deploy all the different channel versions separately from your Windows 10 Enterprise endpoints:

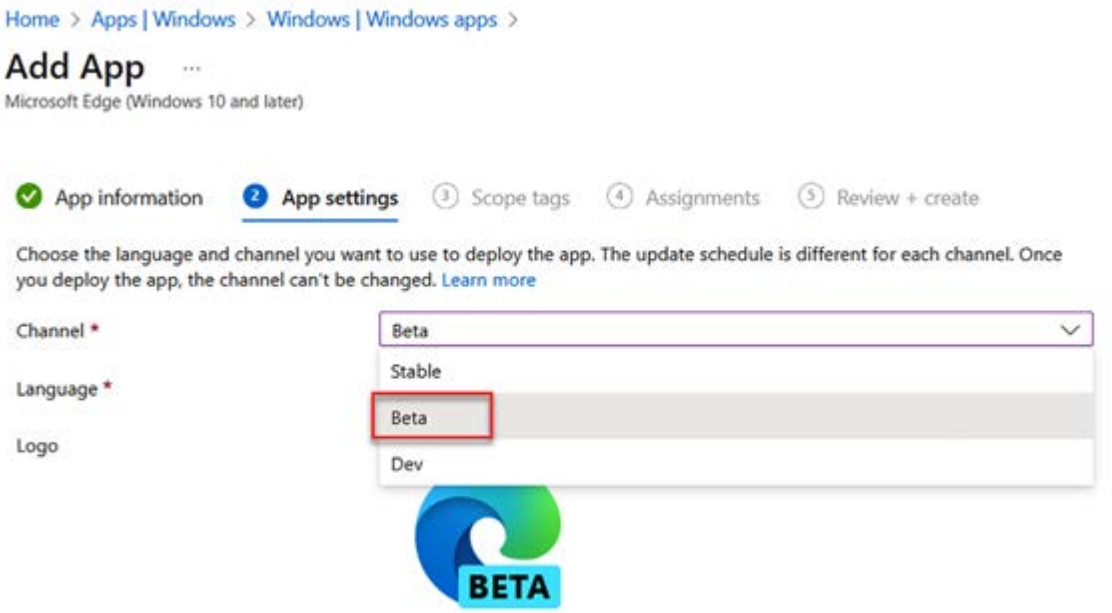


Figure 8.63: Microsoft Edge Beta

The same applies to language settings. Pick the OS default settings when you want to drive language settings from within the Windows OS, or overwrite them when you want to separate the browser language:

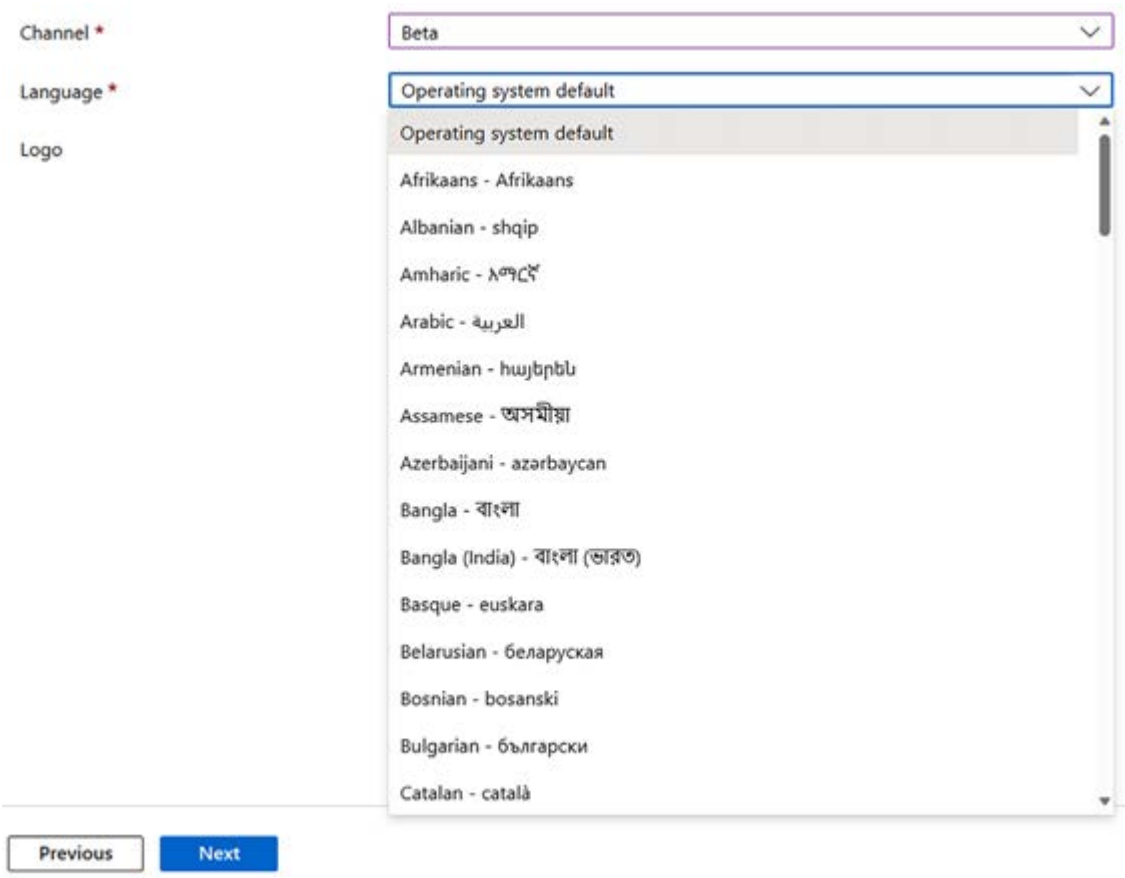


Figure 8.64: Microsoft Edge Language menu

Microsoft Edge is part of every new release of Windows, so this app type will be redundant sometime in the future.

What is WinGet?

WinGet is a command-line tool that enables advanced users and admins to discover, install, upgrade, remove, and configure applications on Windows devices. It is the client interface to the Windows Package Manager service. The tool is designed to make it easier for users to manage their applications and keep them up to date. The tool is available as part of the app installer. If you have already installed the app installer, make sure it is updated with the latest version.

If you are a developer, you can also try the latest Windows Package Manager features by installing a preview build:

- Windows Package Manager v1.6.3421

  The WinGet command-line utility enables installing applications and other packages from the command line:

- Usage: `winget [<command>] [<options>]`

The following commands are available:

- `Install`: Installs the given package
- `show`: Shows information about a package
- `source`: Manage sources of packages
- `search`: Find and show basic info on packages
- `list`: Display installed packages
- `upgrade`: Shows and performs available upgrades
- `uninstall`: Uninstalls the given package
- `hash`: Helper to hash installer files
- `valicdate`: Validates a manifest file
- `settings`: Open settings or set administrator settings
- `features`: Shows the status of experimental features
- `export`: Exports a list of the installed packages
- `import`: Installs all the packages in a file
- `pin`: Manage package pins
- `configure`: Configures the system into a desired state
- `download`: Downloads the installer from a given package

For more details on a specific command, pass it the help argument `[-?]`.

The following options are available:

- `-v,--version`: Display the version of the tool
- `--info`: Display general info about the tool
- `-?,--help`: Shows help about the selected command
- `--wait`: Prompts the user to press any key before exiting

- `--logs,--open-logs`: Open the default logs location
- `--verbose,--verbose-logs`: Enables verbose logging for WinGet
- `--disable-interactivity`: Disable interactive prompts

More help can be found at `https://aka.ms/winget-command-help`.

You can always use **WinGet** to list all installed apps on a device.

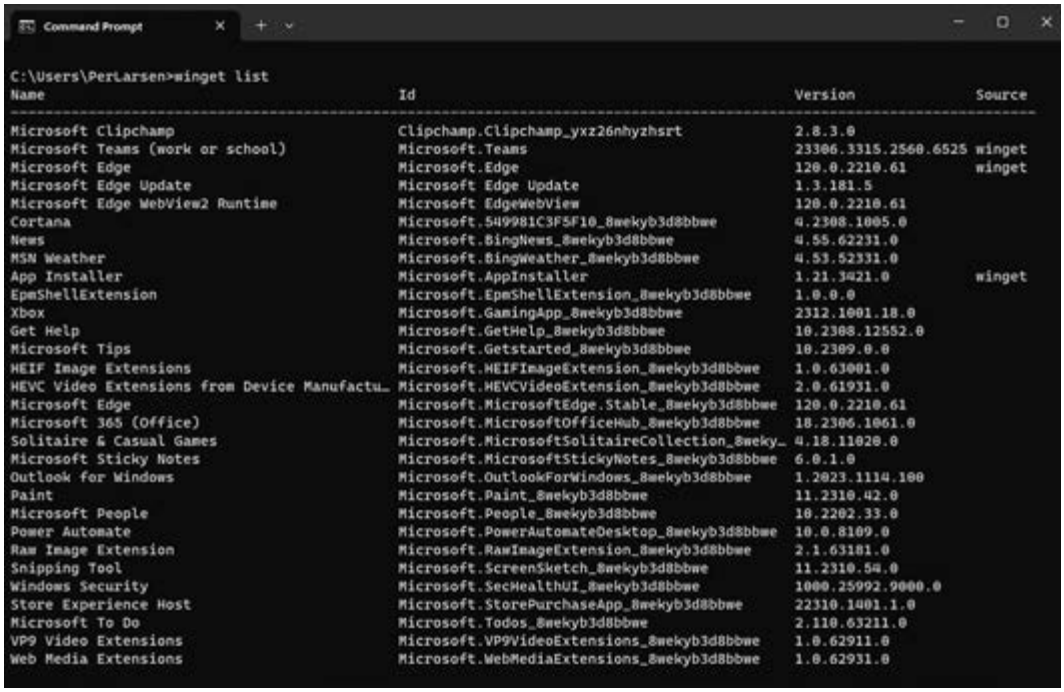


Figure 8.65: WinGet list

You can leverage WinGet to install apps from a command prompt at will.

First, you need to search for the app that you need to find the app that you want to install – in this example, I will find `Vscode`, and as you can see there are multiple options, so I must select the correct `Vscode`, app that I want to install.

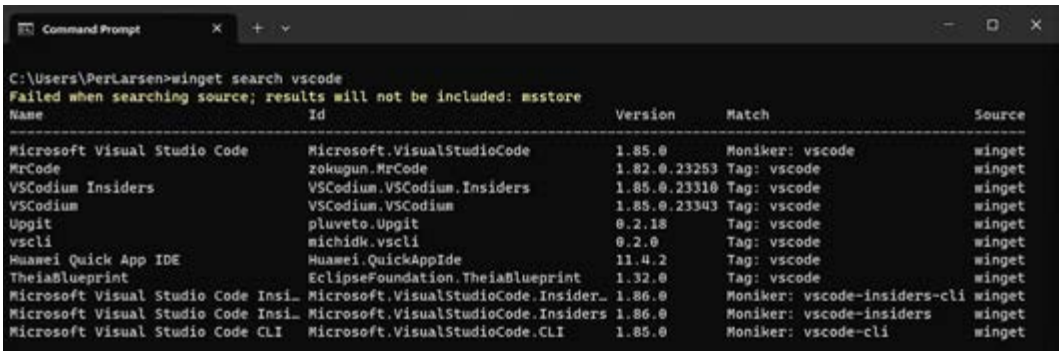


Figure 8.66: WinGet search

I want to install Microsoft Visual Studio Code, so I take the ID (**Microsoft.VisualStudioCode**) and then I run the `winget install` command with the app ID parameter. If it fails to find the app source, you can leverage the source and set it; in this case, the source is set to **winget** where `msstore` is the default repository.

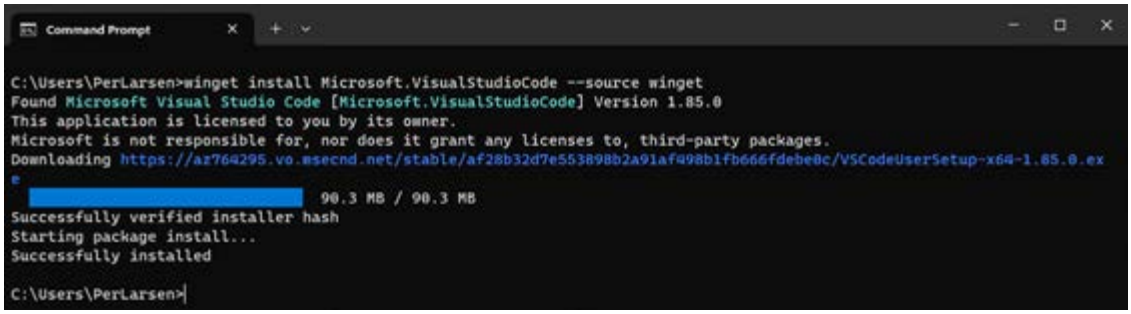


Figure 8.67: WinGet install

After the installation ends, you can start using the installed application. There is always a possibility of creating the app installer as a script and deploying it from Intune.

Sometimes, you just want to source files.

winget search company gives you the app ID `9WZDNCRFJ3PZ`, which you need to download the source files from `msstore`. Now, you can leverage the `download` parameter:

```
winget download 9WZDNCRFJ3PZ -d %temp%
```

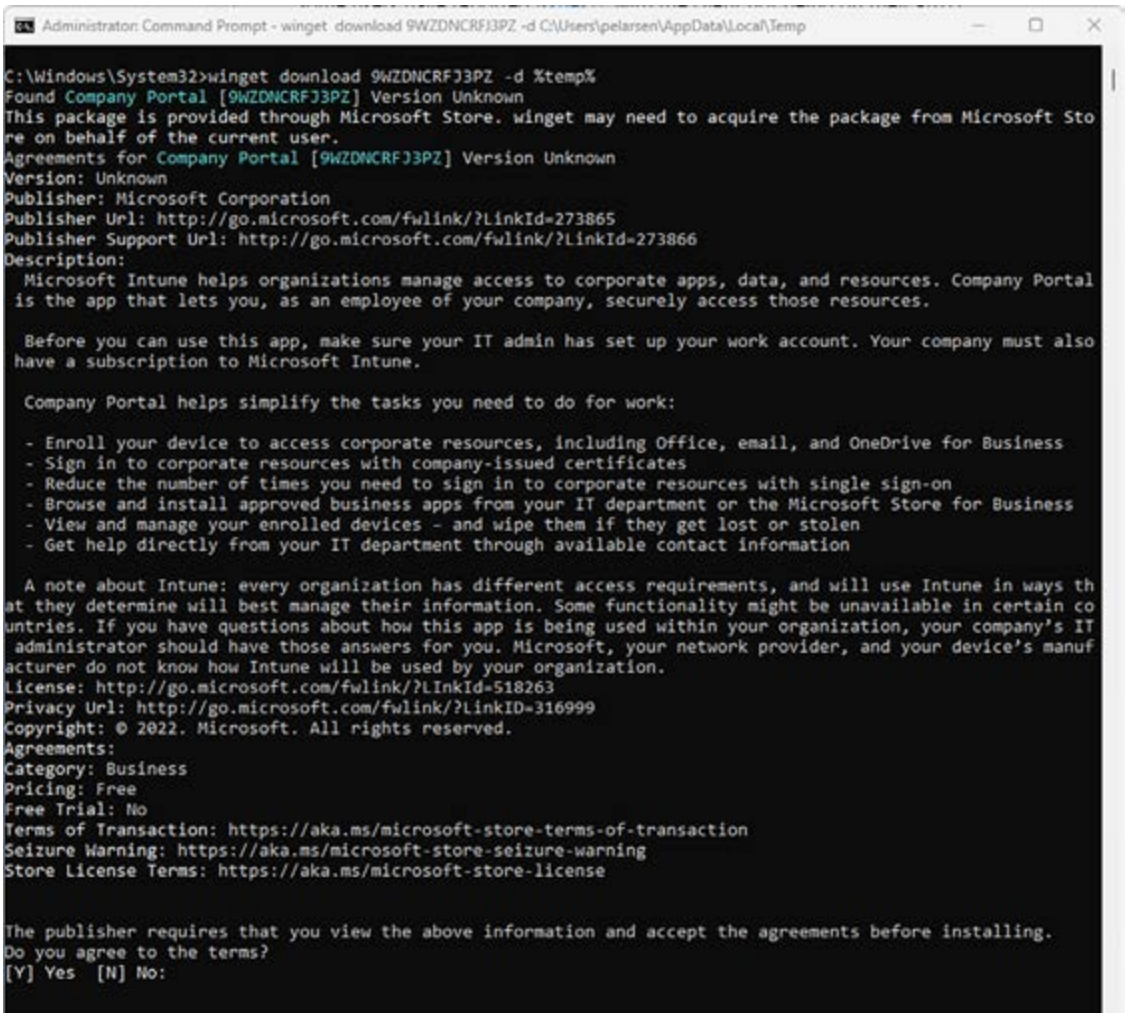


Figure 8.68: WinGet download

When you download a UWP app such as the Company Portal, you can deploy the app as a LOB app with Intune; this applies to HoloLens 2 as well, as a great example.

What is MSIX?

MSIX is a Windows app package format that provides a modern packaging experience to all Win32, UWP, and Windows apps. It's a new way of doing application virtualization compared to technologies such as App-V.

Here are some of the advantages packing an application as MSIX:

- **Simplified installation**: This format eliminates the need for an account with administrative privileges to install, update, or remove the application.
- **Greater security and better performance**: The application installation keeps all application files and registry keys in the application directory (`C:\Program Files\WindowsApps`). This avoids the application compatibility problem, keeps files safe, as it is not possible to change any files or keys in the application directory, and preserves the performance of the OS since the OS files and registry keys are not changed.
- **Access to Windows APIs**: After packaging to the APPX/ MSIX format, the application will have access to all Windows APIs and features such as Windows Hello, Ink, background tasks, toast notifications, or Fluent.
- **MSIX app attach**: This solution can be used on-premises but is recommended for desktop applications installed on **Azure Virtual Desktop** (**AVD**), as it reduces the complexity of managing applications and "golden images" in **AVD**, in addition to reducing host pool storage costs, as each app is made available on **Virtual Hard Disks** (**VHD**). It is based on AVD's application groups, and applications can be instantly available without the need to create new golden images. When FSLogix profile containers and MSIX app attach are used together, the OS remains clean, and data, profiles, and applications are entirely separate.

Separating applications from corporate master images to apply updates and assign applications without doing an image update sounds interesting, right? Well, that's exactly what MSIX can accomplish. Let me explain how you could package an application here:

- Declarative install via the manifest file
- The app signature needs to be trusted on the device
- Tamper protection via BlockMap and signature

- The OS manages the installation, updates, and removal:

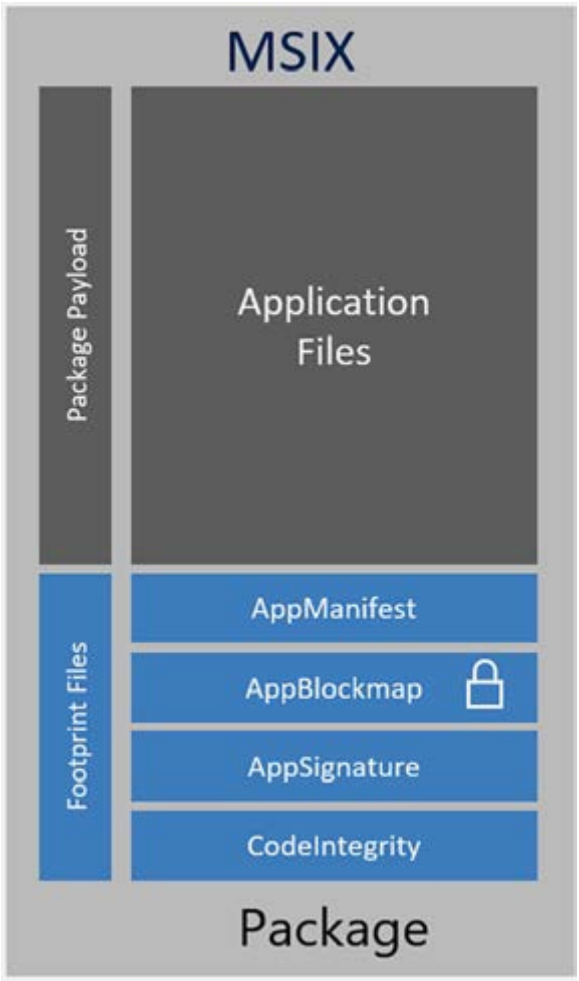


Figure 8.69: MSIX package

AppxManifest.xml

The package manifest is an XML document that contains the information the system needs to deploy, display, and update an MSIX app. This info includes package identity, package dependencies, required capabilities, visual elements, and extensibility points.

AppxBlockMap.xml

The package BlockMap file is an XML document that contains a list of the app's files along with indexes and cryptographic hashes for each block of data that is stored in the package. The BlockMap file itself is verified and secured with a digital signature when the package is signed. The BlockMap file allows MSIX packages to be downloaded and validated incrementally and also works to support differential updates to the app files after they're installed.

AppxSignature.p7x

`AppxSignature.p7x` is generated when the package is signed. All MSIX packages are required to be signed prior to installation. With `AppxBlockmap.xml`, the platform can install the package and it can be validated.

How to create MSIX packages

The process of creating MSIX packages looks pretty similar to what you may have done in the past with App-V. The app developer creates the application and creates the MSIX package (this could be the **independent software vendor** (**ISV**)), after which you customize the application for deployment via Microsoft Intune and assign it to the correct **Azure Active Directory** (**AAD**) group or users.

Let's explain the following steps so you get a good feeling for the process:

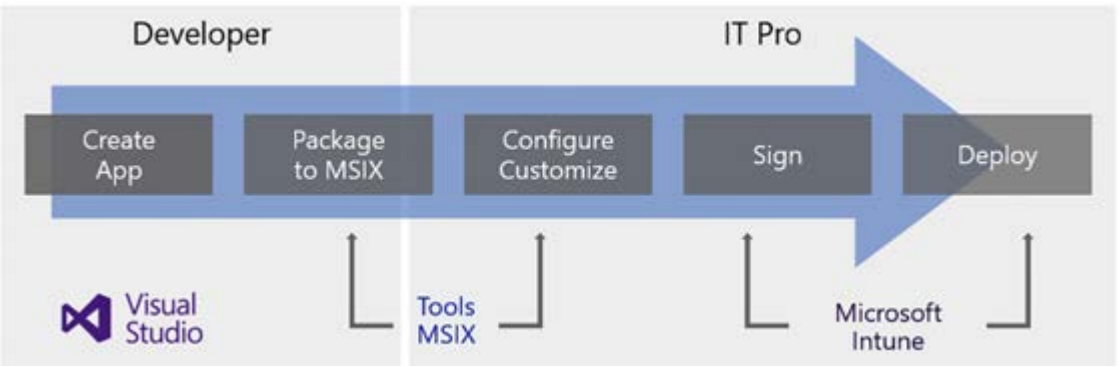


Figure 8.70: MSIX tools

1. First, search for `MSIX Packaging Tool` in the Microsoft Store and install it on your Windows 10/11 virtual machine:

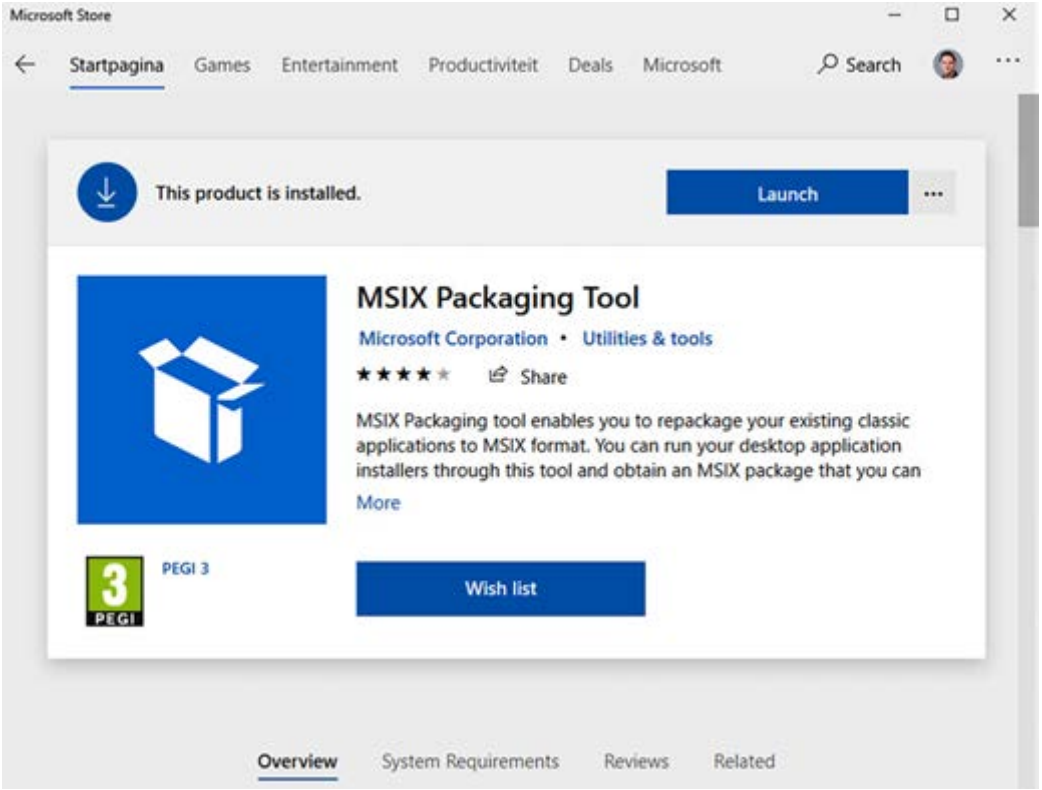


Figure 8.71: MSIX Packaging Tool

2. Start the packaging tool:

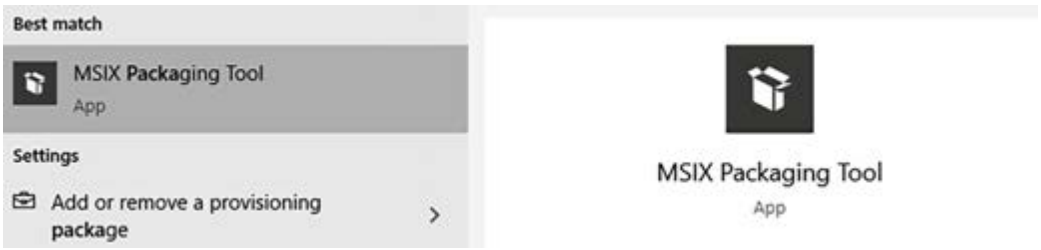


Figure 8.67: Start the MSIX Packaging Tool

3. Click on **Create your app package:**

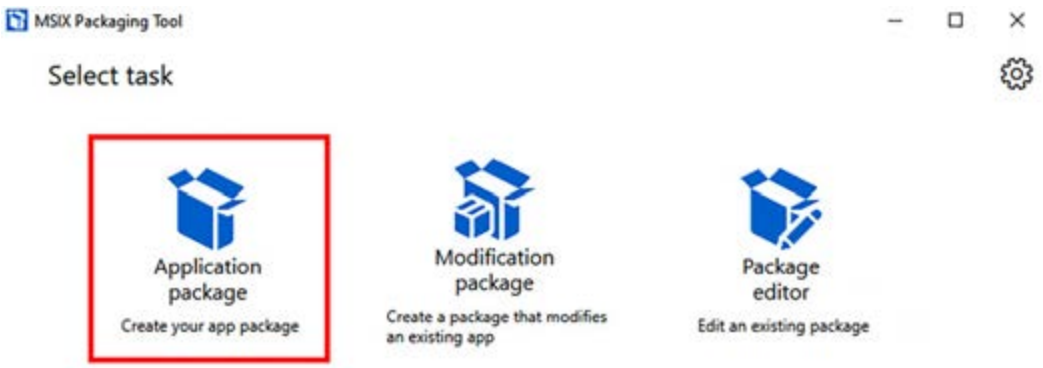


Figure 8.73: Application package

4. Click **Create package on this computer:**

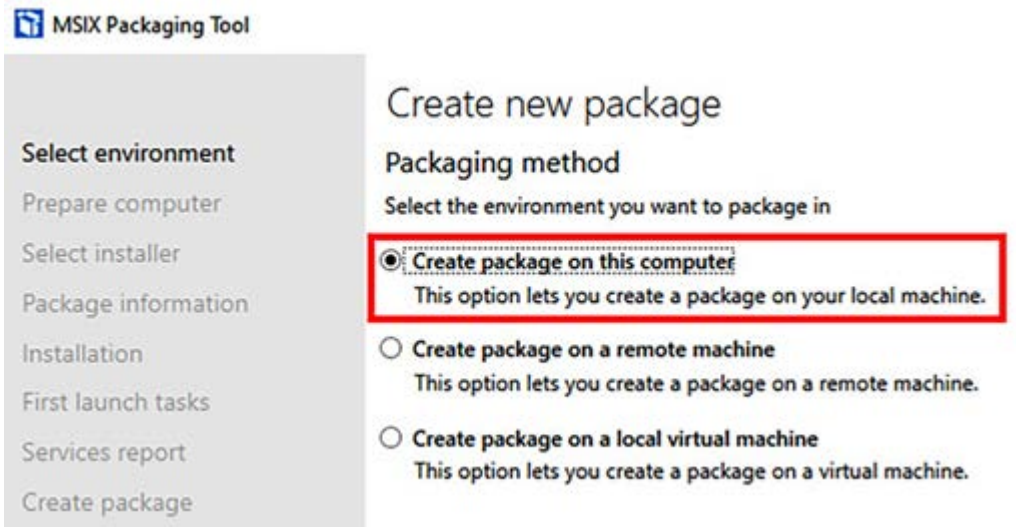


Figure 8.74: Create package on this computer

5. Make sure that the status is the same on your image/session host as in the screenshot for the different action items.

6. Then, click on **Next**:

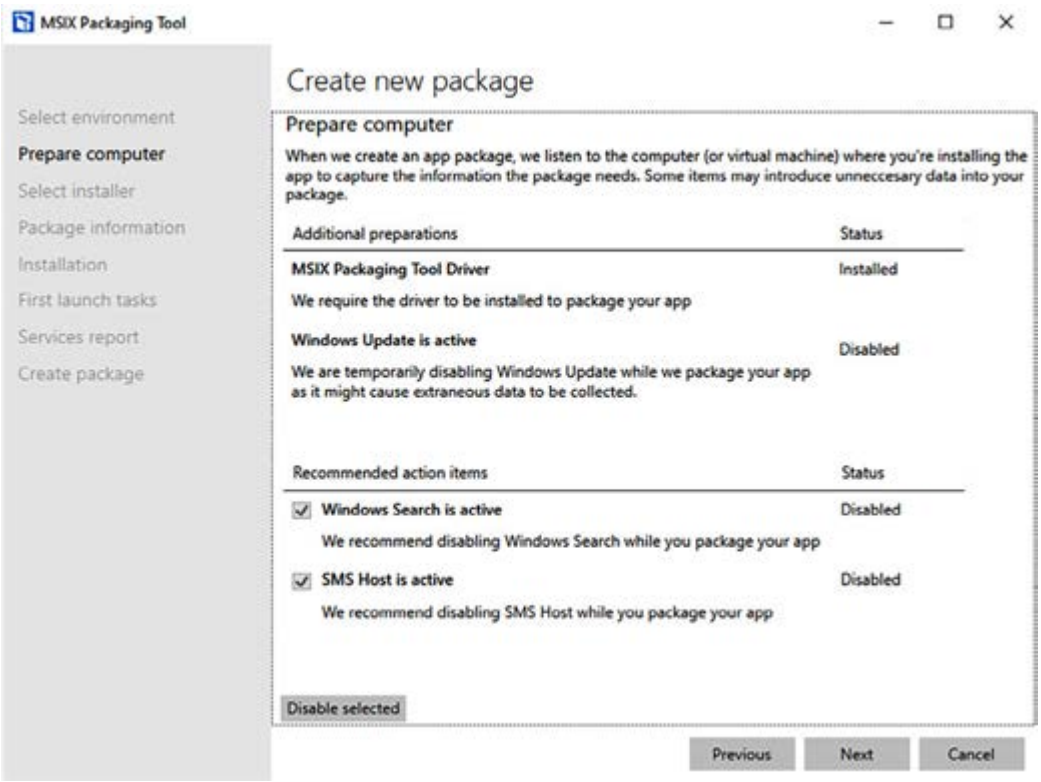


Figure 8.75: Create new package

7. Browse for the application installer. This could be any of your Win32 applications. I'll use Notepad++ for the exercise.
8. Assign your certificate with the correct **Common Name** (**CN**) (for example, `Contoso`), which we will require later. This could be a self-signed certificate as well (for PoC testing purposes):

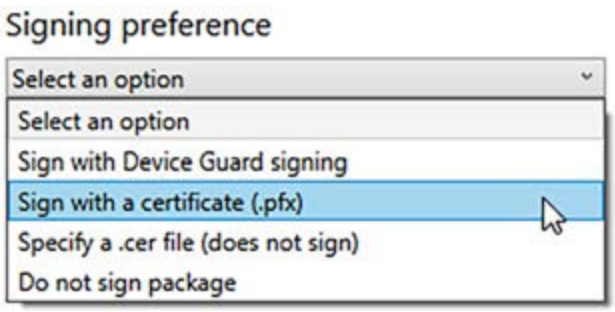


Figure 8.76: Signing preference



MSIX packages must be digitally signed. In order to digitally sign your MSIX package, you can use a self-signed certificate or a developer certificate. You need to ensure that your devices trust the certificate you sign the MSIX packages with; the certificate needs to be imported into the computer's Trusted Root Certification Authorities on the target device where you plan to deploy your MSIX package. If the certificate is not present, your MSIX installation will fail to install.

Make sure that the `CN = Contoso` (organization name) is correct on the certificate as well as in the package configuration.

9. Then, click on **Next:**

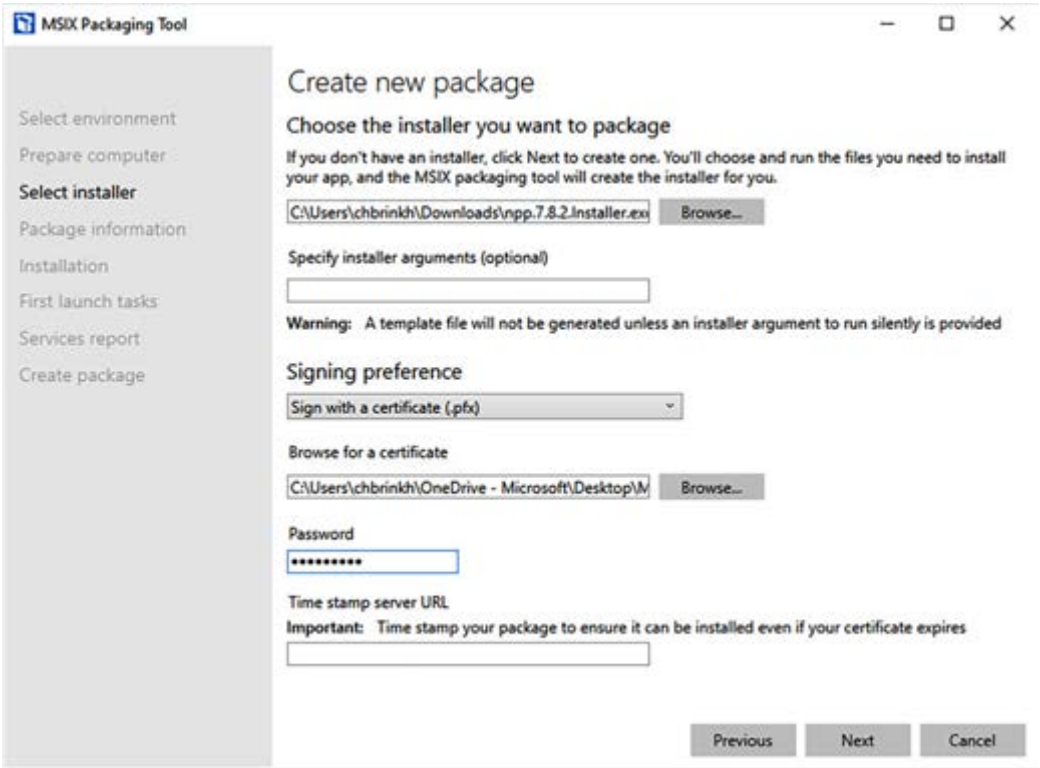


Figure 8.77: Select installer

10. Enter the application-specific requirements. The publisher's name is the certificate CN (for example, `Contoso`) of the organization. Make sure that the certificate is injected into your image, otherwise, the application cannot register and will fail.



If the CN is detected correctly, you'll see the **Subject of the certificate provided** notification. The certificate could be self-signed, public, or internally created via a root CA. The private key and CN must match later in the process.

11. Click on **Next:**

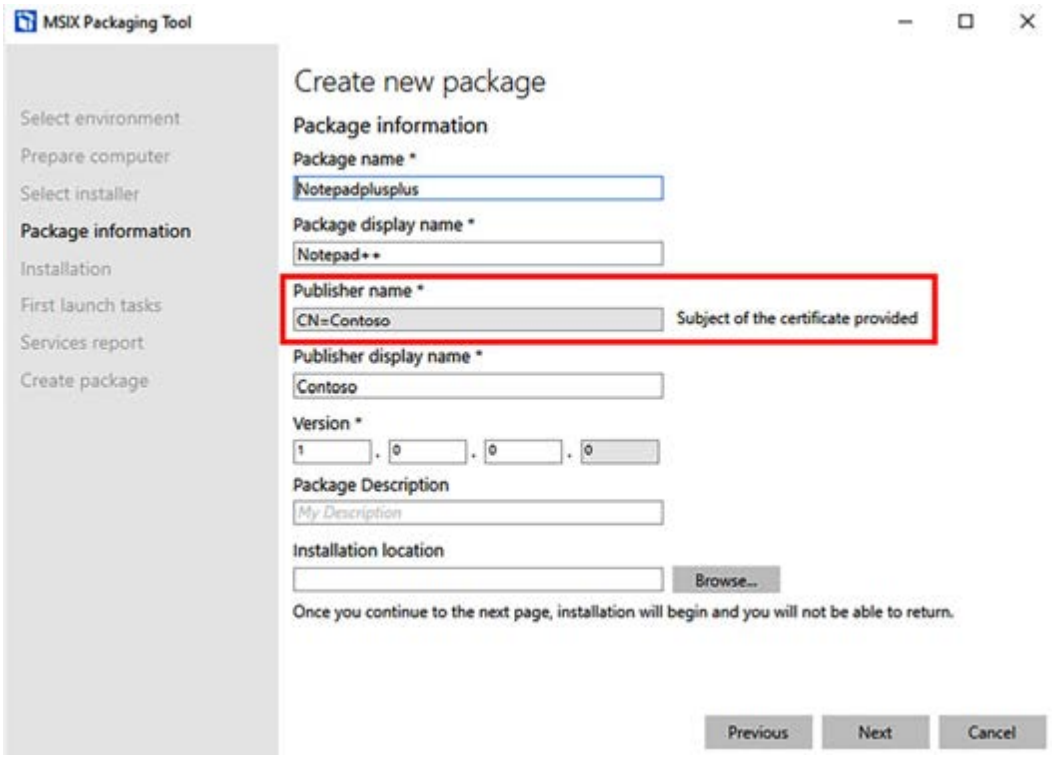


Figure 8.78: Publisher name

12. Now, run through the installation process of your application:

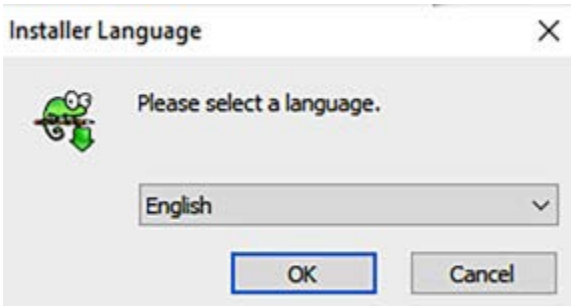


Figure 8.79: Installer Language

13. Make sure to disable **Auto-update** as the MSIX will be read-only.
14. Start the application to make sure that everything has been installed correctly.
15. If the application is installed correctly, you will see the following screen. Make sure to reboot your machine if required before moving on to the next step:

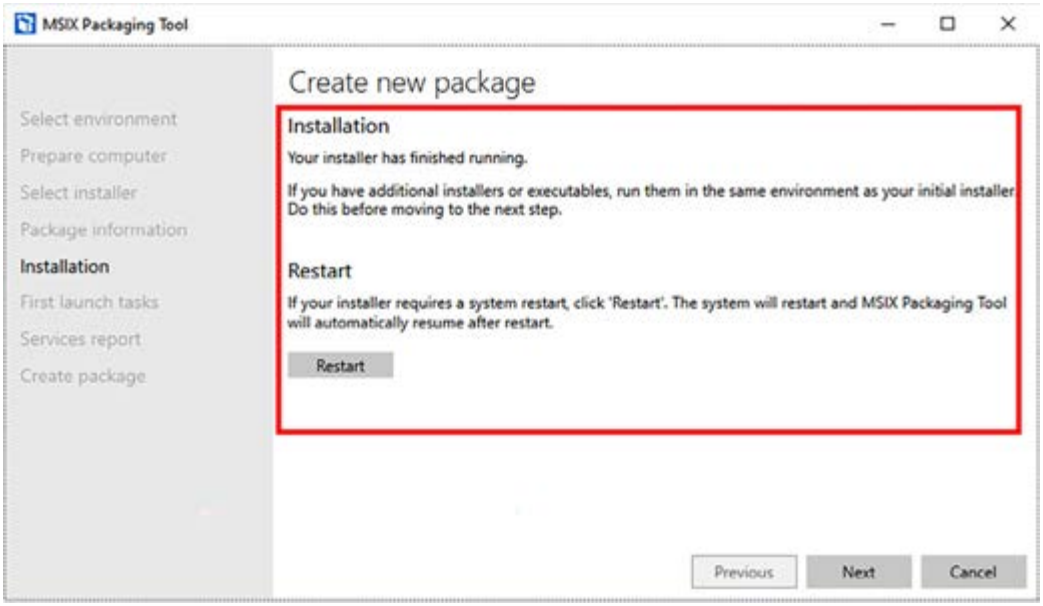


Figure 8.80: Installation

16. We are almost ready. Click on **Next.**



When you want to package extra plugins or other additional applications in the same MSIX package, please click on **No, I'm not done**.

17. I'm done, so I click on **Yes, move on:**

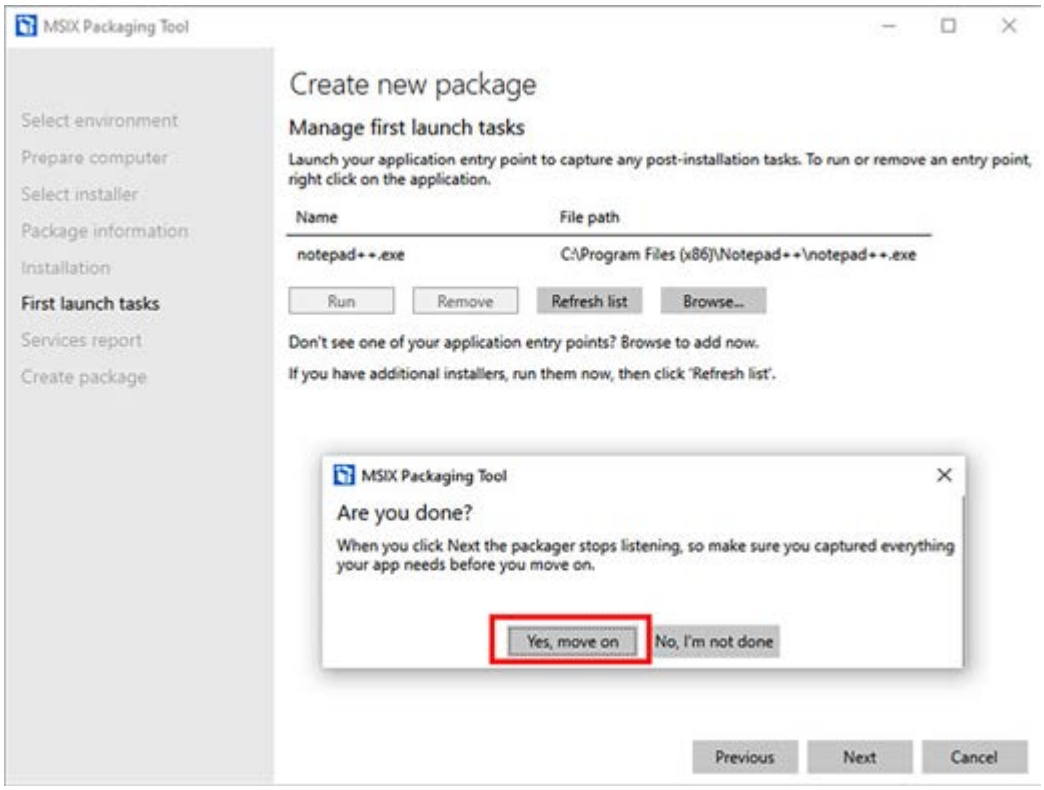


Figure 8.81: Yes, move on

18. Then, click on **Next:**



Figure 8.82: Depends on

19. Save the `.msix` package file somewhere on your computer or network. Then, click on **Create:**

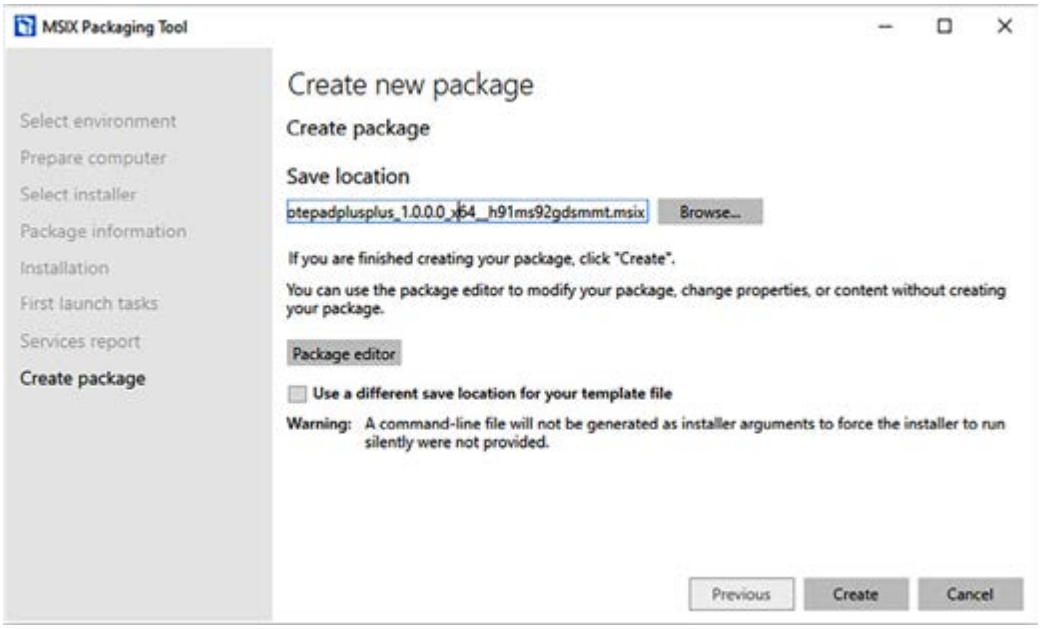


Figure 8.83: Create package

20. The package is ready for the next step. If you want to edit settings in the package, please click on **Package editor:**

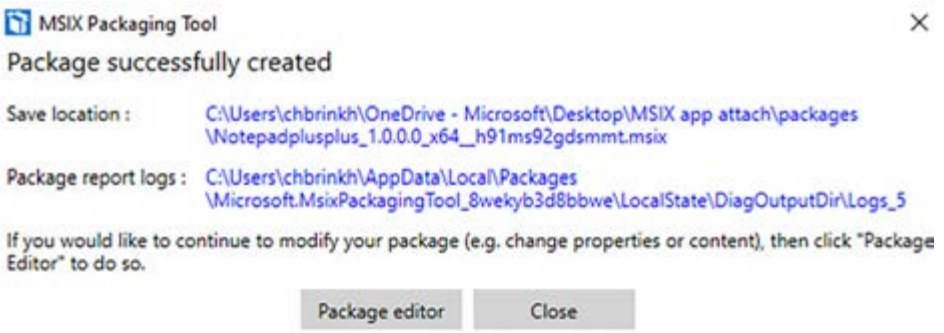


Figure 8.84: Package successfully created

Pushing the MSIX package application to your endpoints

As explained at the start, to deploy MSIX applications, you must use **Line-of-business app** as the **App type** setting:



The deployment of MSIX happens via the Intune Sidecar agent.

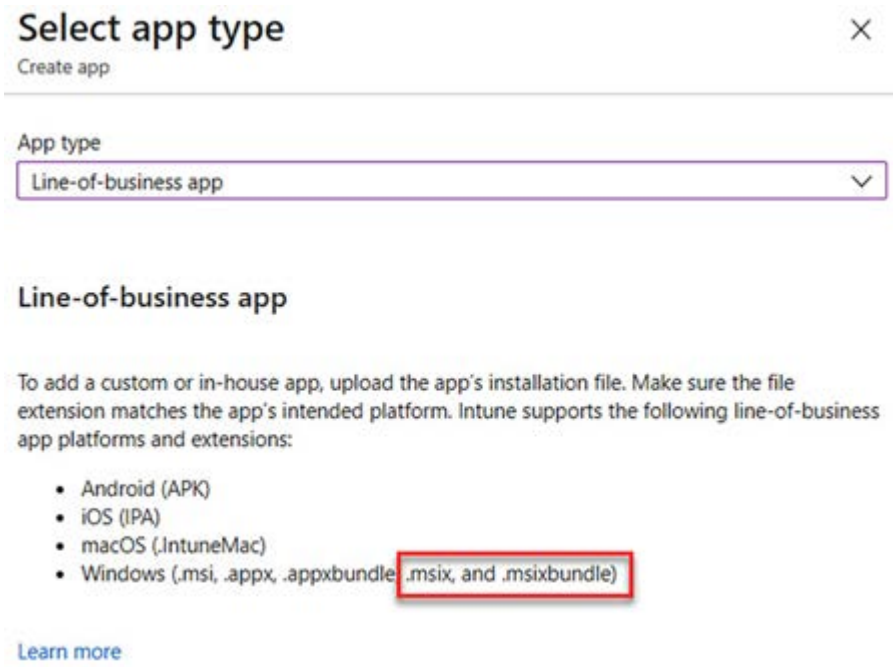


Figure 8.85: LOB MSIX

It will prompt you for the `.msix` package file that will be uploaded to Microsoft Intune and distributed to your Windows 10 Enterprise endpoints:

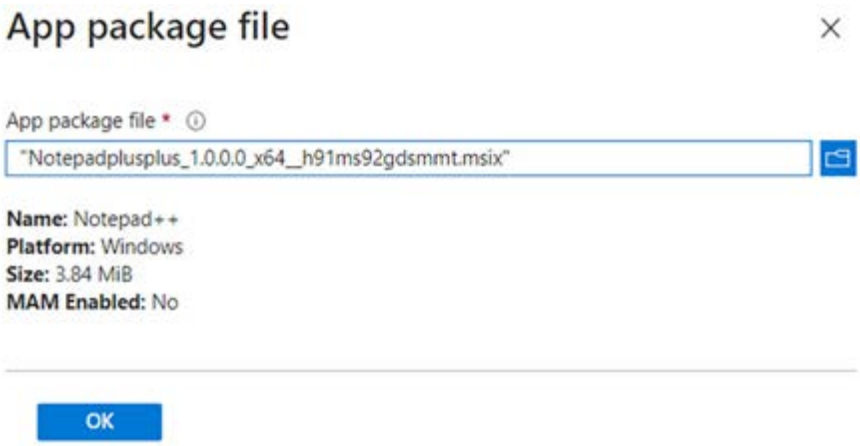


Figure 8.86: MSIX App package file

The application settings are pretty much the same as for other application formats – very straightforward:

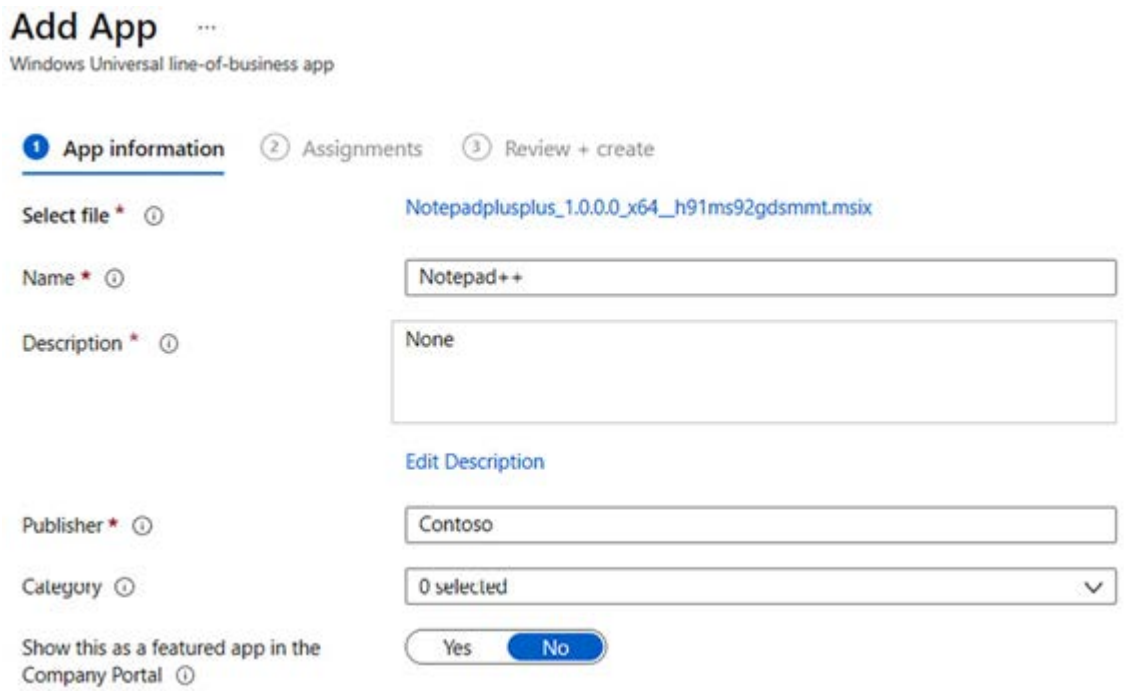


Figure 8.87: App information MSIX

Once done, you should assign the MSIX application to the correct AAD groups and the application will be injected inside Windows 10 Enterprise without installing it:

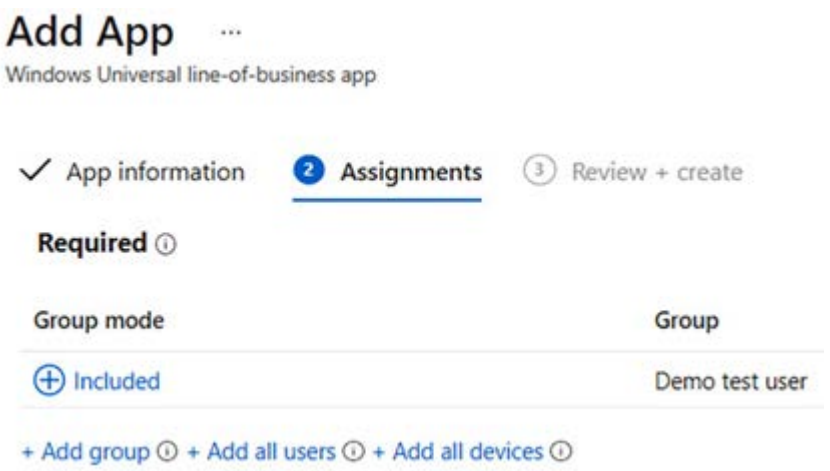


Figure 8.88: App Assignments MSIX

Are you looking for easy ways to migrate apps from Configuration Manager to Microsoft Intune on a large scale, completely automated, while also doing a conversion to Intune packages? Rimo3 modernizes your application estate. From migration to maintenance, Rimo3 is a solution that automates pre-production compatibility testing, package modernization, and migration of your Windows application estate. It is used to test and modernize applications for OS upgrades, patch updates, migrations from legacy to cloud workspaces, modern management planes, and ongoing maintenance for evergreen environments.

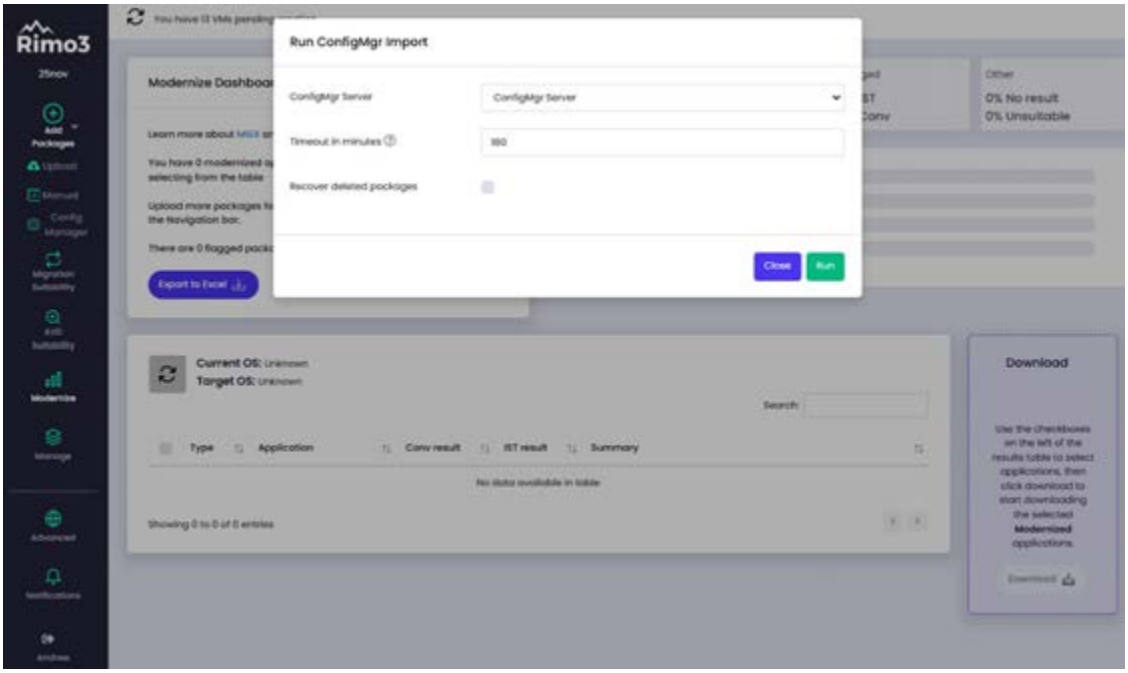


Figure 8.89: Run ConfigMgr Import

This concludes the section regarding application virtualization with MSIX and delivery to your endpoints with Microsoft Intune. There is no need to switch to the Azure portal – everything is consolidated for a unified management experience.

Summary

In this chapter, you've learned about all the different options to configure and distribute applications as regards both your physical and cloud endpoints. As this is a very important factor of the modern desktop, you are one step closer to becoming a modern workplace rockstar.

In the next chapter, we will deep dive into another important element of the modern desktop, which is policy management!

Questions

1. What is the preferred and most comprehensive application deployment type for Windows applications (Win32)?
    a. LOB app
    b. Windows app (Win32)
    c. Web link
    d. Microsoft Store app
2. What is the Edge release channel called for production usage workloads?
    a. Canary
    b. Stable
    c. Dev
    d. Beta

Answers

1. (b)
2. (b)

Further reading

If you want to learn more about Microsoft Intune application deployment options, please use one of the following free online resources:

- Windows 10 app deployment by using Microsoft Intune | Microsoft Docs: `https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy`
- Assign apps to groups with Microsoft Intune | Microsoft Docs: `https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy`

Join the CloudPro Newsletter with 44000+ Subscribers

Want to know what's happening in cloud computing, DevOps, IT administration, networking, and more? Scan the QR code to subscribe to **CloudPro**, our weekly newsletter for 44,000+ tech professionals who want to stay informed and ahead of the curve.

`https://packt.link/cloudpro`

9

Understanding Policy Management

In this chapter, you will learn about how policy management from Microsoft Intune is different from **Group Policy Objects** (**GPOs**) and the different policy types in Intune that give you various options to customize and secure the Windows Enterprise desktops in your environment. This chapter will be very broad in terms of content, but it will give you the basic information needed to understand how policy management works between Windows and Microsoft Intune.

We have divided policy management into three chapters in this book, and the following one is the first one – *Chapter 10*, *Advanced Policy Management*. That chapter deals with advanced policy management with different scenarios. In this chapter, we'll cover the following topics:

- Policy management
- What is a **Configuration Service Provider** (**CSP**) policy?
- **Windows Push Notification Service** (**WNS**)
- Getting started with policy design
- Policy management within Microsoft Intune
- Migrating existing policies from **Azure Directory** (**AD**) – Group Policy management

Policy management

Using Microsoft Intune to manage your Windows Enterprise desktops is all about standardizing and simplifying the management layer of your environment. As explained in the previous chapter, everything is centered around structuring your configuration sets (and applications) separately from the target **Operating System** (**OS**) to remove the need to create custom images that might include these things from the get-go.

Policy management within Microsoft Intune makes it possible to configure the following options from within the **Devices** menu:

- Compliance policies
- Conditional access
- Configuration profiles
- Settings catalog
- ADMX import
- Scripts
- Group policy analytics
- Enrollment restrictions

Group Policy management has been around for more than 20 years and is a way to configure the behavior of a group of users or computers in a domain. This is still possible with an on-premises domain today, but if you want to start modernizing your policy and settings management, you should start looking at Microsoft Intune and the feature set it provides for policy management. There are some disadvantages associated with using GPOs, one of them being that it requires a line of sight to a domain controller. Another is that GPOs are fire-and-forget, but what do we mean by this? GPOs are assigned to a specific group of users and devices, and they are applied when a device connects to a domain controller on a regular basis. There is no reporting back to the domain controller if the device receives and applies the policy correctly, if no domain controller can be contacted, or if no new or changed policies are applied.

Sometimes, due to misconfiguration, a Windows device may try to contact a domain controller far away on the internal network with very slow connectivity, which can result in very long boot and sign-in times. Many of these issues can be avoided with a purely cloud-joined and -managed device.

Microsoft Intune is a perfect match for a new way of working guided by modern management and cloud-native, as it just requires internet connectivity following the initial onboarding into Microsoft Intune.

In this chapter, we will focus on cloud-native devices, that is, Enrtra-joined and Intune-managed Windows devices, but what we learn will also apply to hybrid domain-joined devices that are managed from Microsoft Intune in a co-managed state. One important thing to note here is that GPO and **Mobile Device Management** (**MDM**) settings are on the device identity layer, where policies and configurations are either target users or devices, whereas co-management between Microsoft Intune and **System Center Configuration Manager** (**SCCM**) is on the management plane.

First, we need to look back at traditional Windows management, where all Windows devices were on-premises in the office, in production, or with end users working at home with VPNs. Modern policy management is still an option on those devices if they are hybrid-joined to Entra ID.

The best option moving forward with new devices is to go purely Entra-joined and onboarded with Windows Autopilot. What we cover in this chapter covers both scenarios. This book is dedicated to cloud management, and certain scenarios do not apply to hybrid-joined devices, which is why you need to make some decisions to go to Entra-joined devices to get the best end-user experience. Start small, start with a **Proof of Concept** (**POC**), and showcase the benefits of modern policy management. A best-practice approach is to block on-premises devices in your POC from getting GPOs from the local Active Directory instance; otherwise, you can end up in a situation where you are not 100% sure where the settings are being applied from.

A **Configuration Service Provider** (**CSP**) is an interface for reading, setting, modifying, and deleting configuration settings on a device. These settings map to registry keys or files. Some CSPs support WAP format, some support SyncML, and some support both. SyncML is only used over the air for **Open Mobile Alliance Device Management** (**OMA DM**). On the other hand, WAP can be used over the air for OMA client provisioning, or it can be included in a phone image as a **.provxml** file that is installed during boot.

What is a CSP policy?

Some policies can only be configured at the device level, whereas other policies can be configured at the user level. This means that device-level policies will have an effect independent of the user logging in to the device, whereas user-level policies will only have an effect depending on the user logging in to the device. As an example, different users can have different homepages in Microsoft Edge, so it is appropriate to assign a policy with that setting to a user group, whereas security settings that need to be applied at the device level are appropriate to assign to device groups.

User scope is where the policy only applies to the user who logs in to the device, and the policy can vary depending on who is logging in to the device. The following is an example of what the CSP tree looks like when configuring a user policy:

- `./User/Vendor/MSFT/Policy/Config/AreaName/PolicyName` is used to configure the policy.
- `./User/Vendor/MSFT/Policy/Result/AreaName/PolicyName` is used to get the result.

Device scope is where the policy only applies to the device itself, regardless of the user who logs in to the device. The following is an example of what the CSP tree looks like when configuring a device policy:

- `./Device/Vendor/MSFT/Policy/Config/AreaName/PolicyName` is used to configure the policy.
- `./Device/Vendor/MSFT/Policy/Result/AreaName/PolicyName` is used to get the result.

The biggest difference between a GPO and a CSP policy is that a CSP policy has a result channel as well, so every setting that is configured on the device will report back to the MDM system – in this case, Microsoft Intune.

If we take a closer look at the policy structure, it looks like the Windows registry is arranged in a tree structure:

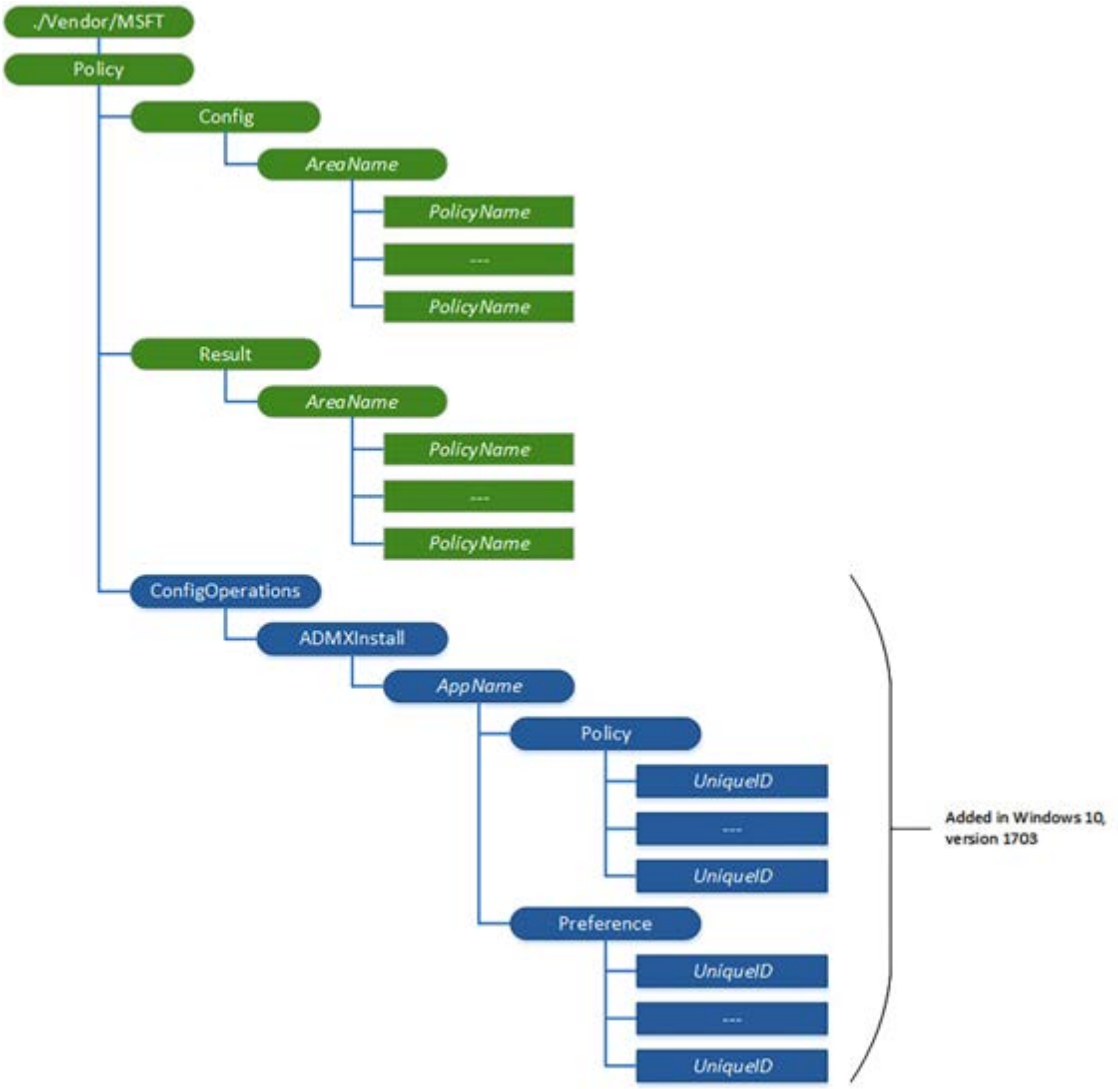


Figure 9.1: CSP policy tree

By using ADMXInstall, you can add ADMX-backed policies for those Win32 or Desktop Bridge apps that have been added between OS releases. ADMX-backed policies are ingested by your device by using the CSP policy URI: `./Vendor/MSFT/Policy/ConfigOperations/ADMXInstall`.

The OMA-URI string needs to go into the CSP policy URI:

- `./Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/Applicationname/Policy/ADMXFileName`.

- `./Vendor/MSFT/Policy/Config/` remains the same for all machine-based policies that you deploy to the device.

Applicationname and **ADMXFileName** are user-defined. In this case, **Applicationname** is **App1**, and you can use the same name as **ADMXFileName**. Just remember that **ADMXFileName** needs to be unique, which means you cannot deploy two ADMX files with the same name on a device, as it will fail and any additional ADMX files will not be added to the device.

Here is the content of the ADMX file in my case – this could also have been Google Chrome, Microsoft Office, Internet Explorer, or others:

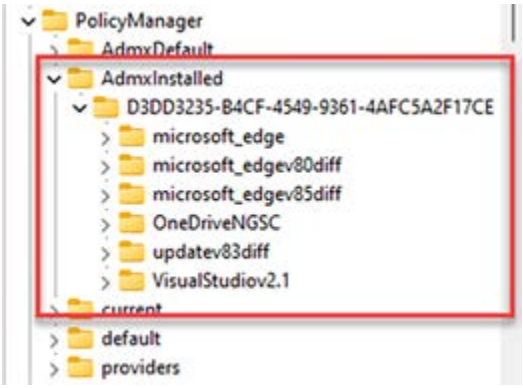


Figure 9.2: Registry entry for AdmxInstalled

Then, if you take a closer look at the registry, the first place where they are written is `HKLM\SOFTWARE\MICROSOFT\PolicyManager\AdmxInstalled`.

The policy is always declared under a GUID and with the name you gave the policy in Microsoft Intune when you created the policy.

Then, you will be able to see the naming of the policy category that you are using when creating a policy setting: `HKLM\Software\Microsoft\PolicyManager\AdmxDefault`

If the policy is a device policy, you will be able to see the direct results that apply to the devices in the following location: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device`.

In the end, all a policy does on a Windows device is set some registry keys, and it is the same with MDM policies. All the policy settings go here: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\`.

MDM policies are applied when a device syncs, either from Microsoft Intune or as part of the 8-hour schedule when a Windows device is running with MDM sync on.

For an IT admin to sync a device from Microsoft Intune, they need to start the Microsoft Intune admin center and follow these steps:

1. Click **Home** | **Devices** | **Windows** | **Windows devices**.
2. Search for the device you want to sync, and then select the device and click **Sync**. Intune will then try and reach out to the device through **Windows Push Notification Service** (**WNS**).

3. You can read more about WNS in the next section.



Figure 9.3: Device sync

4. In the same view, where you just selected a single device, you can also leverage **Bulk Device Actions:**



Figure 9.4: Bulk device actions

5. Select **Windows** for **OS.**
6. For **Device type**, select **Cloud PCs** or **Physical devices.**
7. Select **Sync** as **Device action:**



Figure 9.5: Bulk device action – Windows

8. Then, you can select up to 100 devices that Microsoft Intune will reach out to and perform the sync:

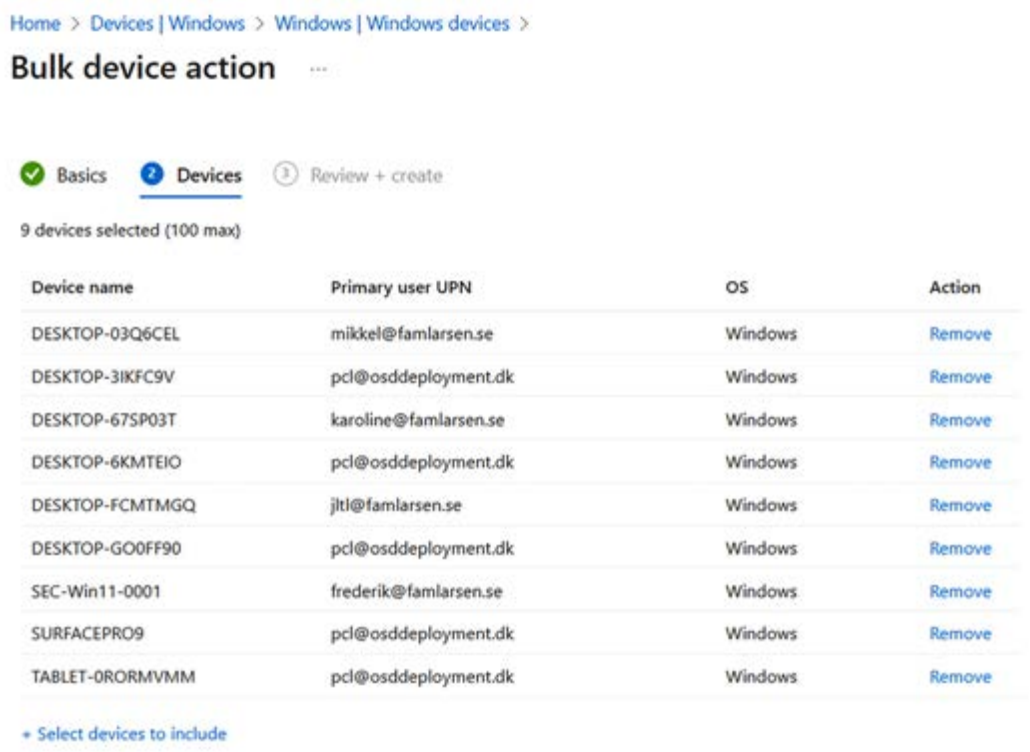


Figure 9.6: Bulk device action

When leveraging bulk device actions, Microsoft Intune uses WNS. In the next section, you will learn about how WNS works.

Windows Push Notification Service (WNS)

WNS enables Microsoft Intune to send toast, tile, badge, and raw updates from Microsoft Intune to MDM-enrolled devices. This provides a mechanism to deliver new updates to your users in a power-efficient and dependable way:

1. Microsoft Intune makes an **HTTP POST** to the channel URI. This request is made over SSL and contains the necessary headers and the notification payload.
2. WNS responds to indicate that the notification has been received and will be delivered at the next available opportunity.

WNS does not provide end-to-end confirmation that your notification has been received by the device or application. Microsoft Intune provides this option by showing the status in the **Device actions** status view on the **Overview** blade for a specific device:

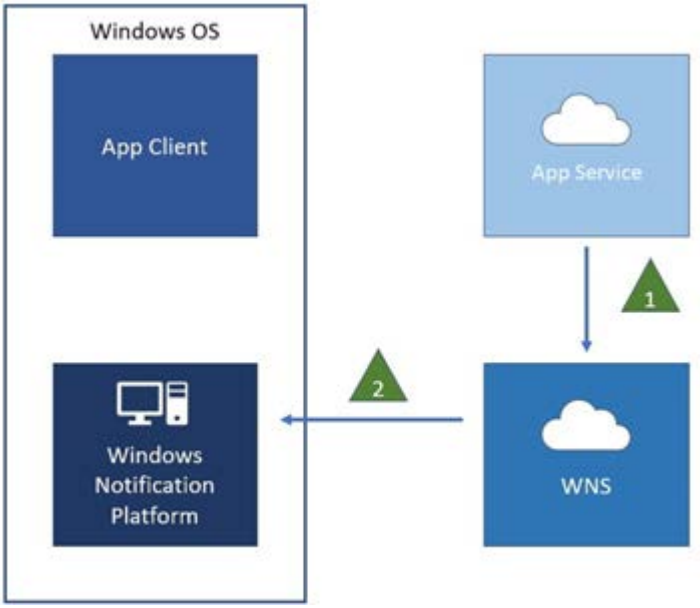


Figure 9.7: WNS workflow

3. There is also an option for an end user to do this from the client side. On the client side, you can do a sync from **Company Portal** or the settings app.
4. In the Start menu, you can search for **Company Portal** (we recommend that IT admins always push Company Portal to the end user's Windows device), which will give you the option to sync this device:

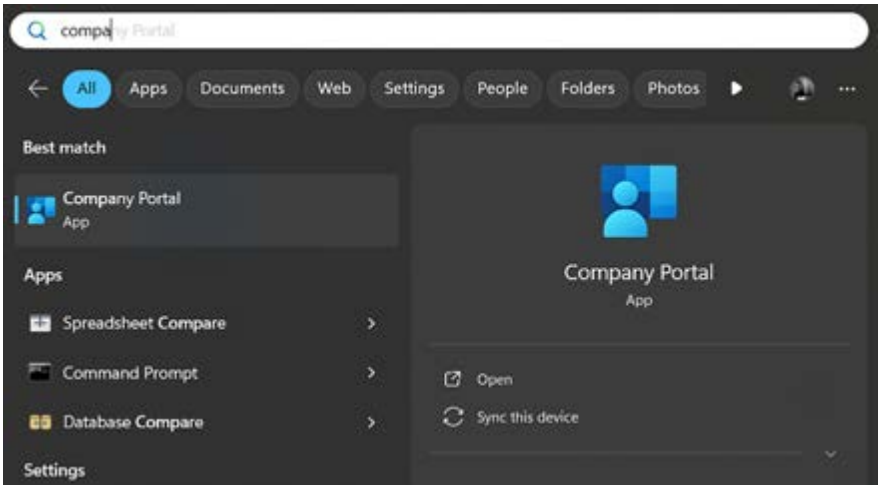


Figure 9.8: Company Portal

5. If **Company Portal** is pinned to the Start menu, you can right-click and sync this device:

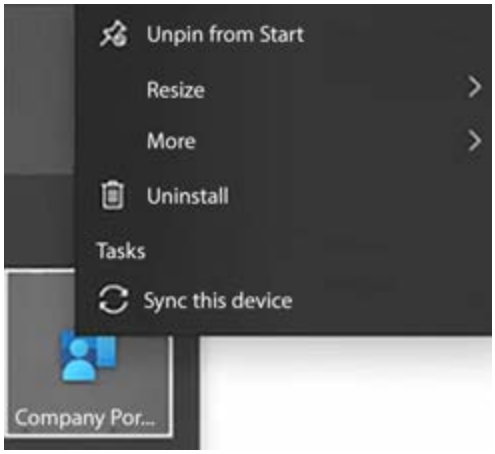


Figure 9.9: Sync this device

6. In **Company Portal**, go to settings, and then click **Sync:**

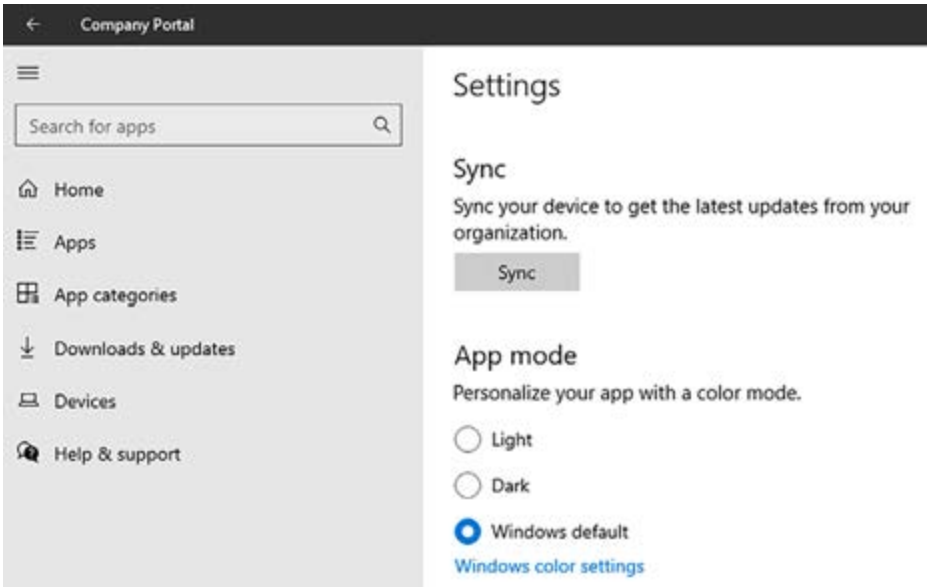


Figure 9.10: Manually sync your device

7. In the Windows settings app, you can go to **Accounts** | **Access work or school.**
8. Select the identity from Entra ID, and then click **Info.**
9. You are then able to see the policy areas managed by your company.

On Windows 11, you also have the same option as on Windows 10, but you can perform an export of your management log files directly from the **Access work or school** page in the Settings app:

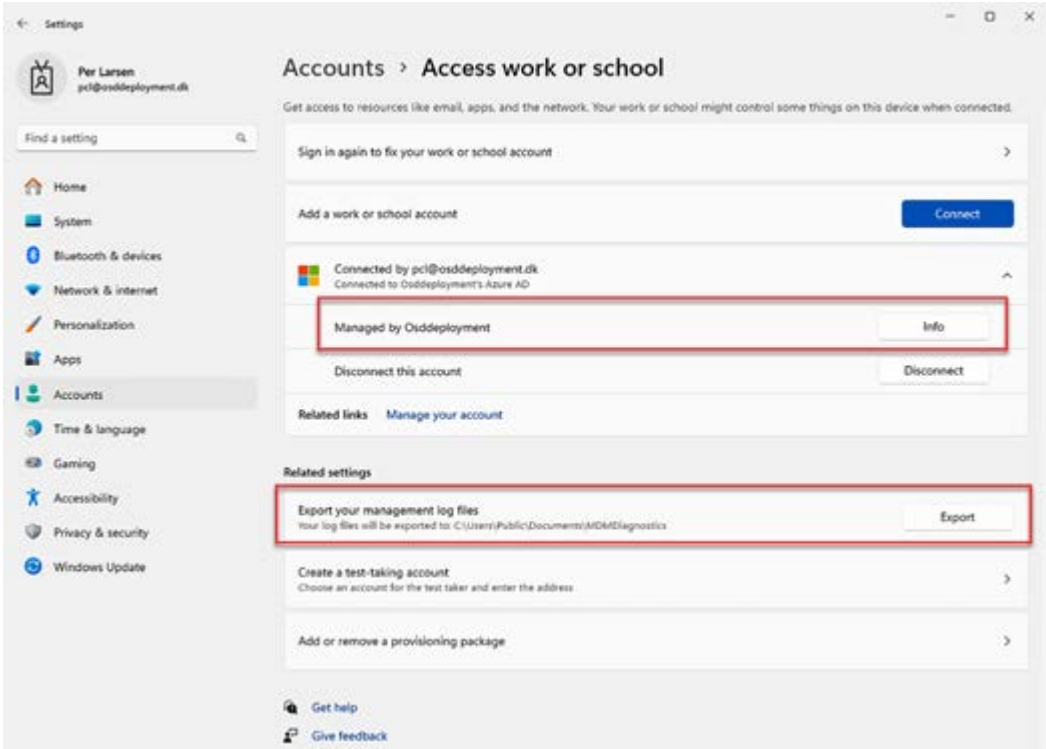


Figure 9.11: Managed by your company

10. When you click **Info**, you will get a more detailed page:

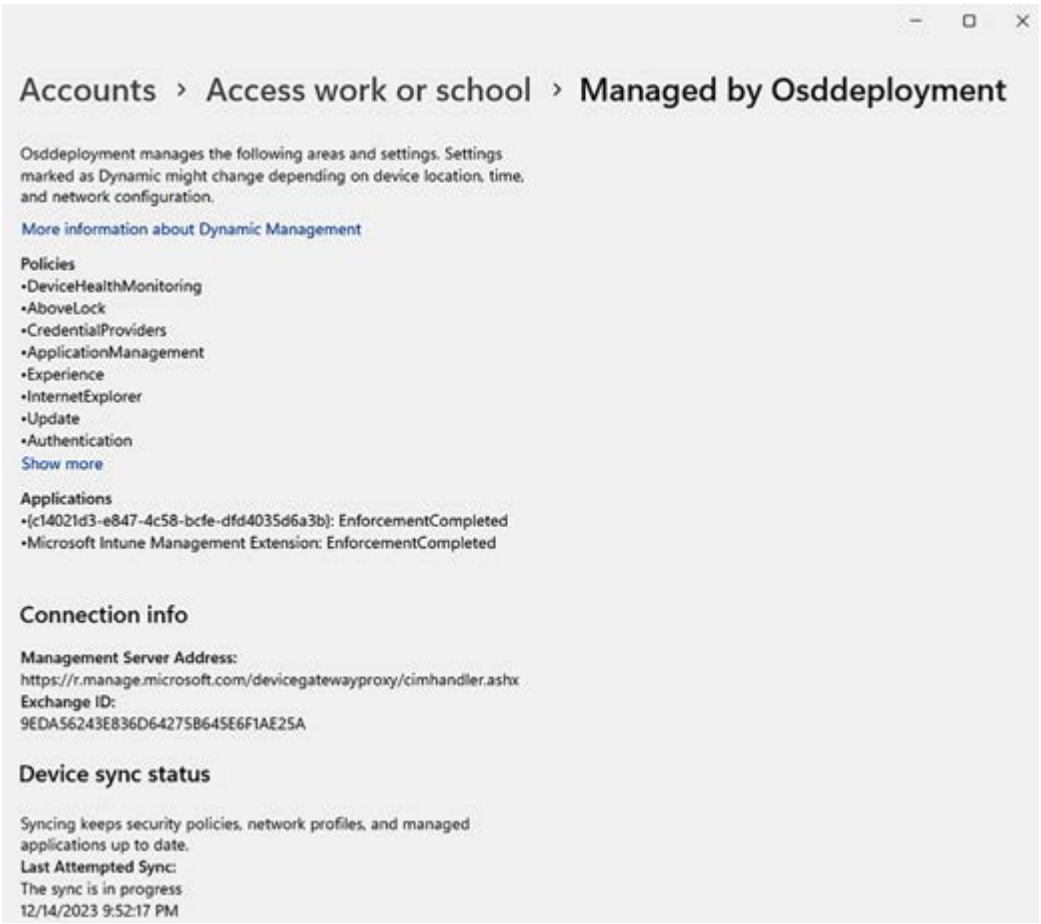


Figure 9.12: Managed by your company

11. If you scroll to the bottom of this Settings page, you will see **Device sync status**, where you can see **Last Attempted Sync** and the **Sync** button:

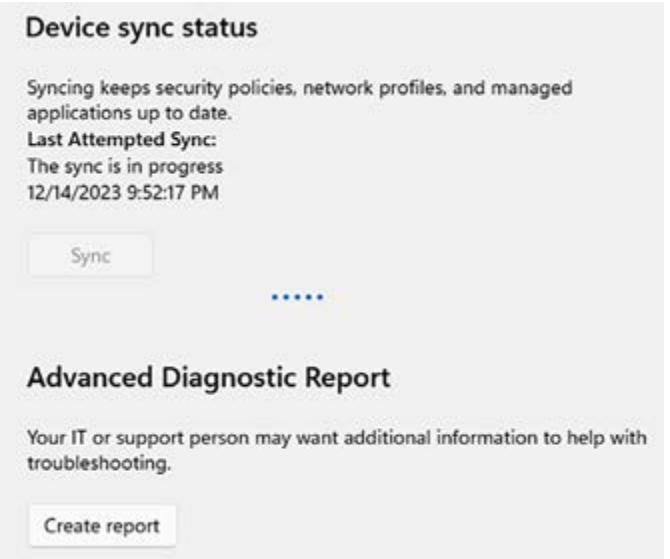


Figure 9.13: Device sync status

When a user is doing an MDM sync, all new policies will be applied to the device and it will be verified that all existing policies have been applied.

That concludes this section on WNS and MDM synchronization. In the next section, we will cover getting started with policy design in Microsoft Intune.

Getting started with policy design

When designing your strategy for policy management with Microsoft Intune, it is important to take the right approach.

By starting with a security baseline, we get well-tested and secure sets of policies; you can even disable or remove individual settings in the security baseline if they do not suit your organization. When you have deployed the security baseline, you can start adding other policy types that suit your security or configuration needs.

There are several policy types in Microsoft Intune. In the following list, you can see the different policy types and the order in which you should start creating policies:

1. Configure the security baseline.
2. Configure the policy from the **Endpoint Security** blade.
3. Configure the policy from the **Settings** catalog.
4. Configure the administrative template.
5. Configure the device configuration.
6. Leverage a custom policy as a last resort.

Just remember that there are no right and wrong approaches, but if you're undertaking a migration from Active Directory GPOs to MDM settings management, it might be a good time to start afresh and see what you need to configure instead of taking the legacy GPO settings of your on-premises environment with you. Sometimes, organizations do not even know why they implemented a specific policy setting back when they originally created it. Perhaps the person responsible for implementing this policy setting is no longer even with the company and did not leave any documentation on why the setting was configured the way it was in the first place.

As there is no conflict handling in the MDM stack, you might inadvertently create a conflict between two settings coming from two different policies to the same user or device. These could be from the same policy type or different policy types, so it is important to spot and monitor any conflicting policies.

1. In order to monitor any conflicting policies, head to the Microsoft Intune admin center, and under each device, go to **Home | Configuration:**

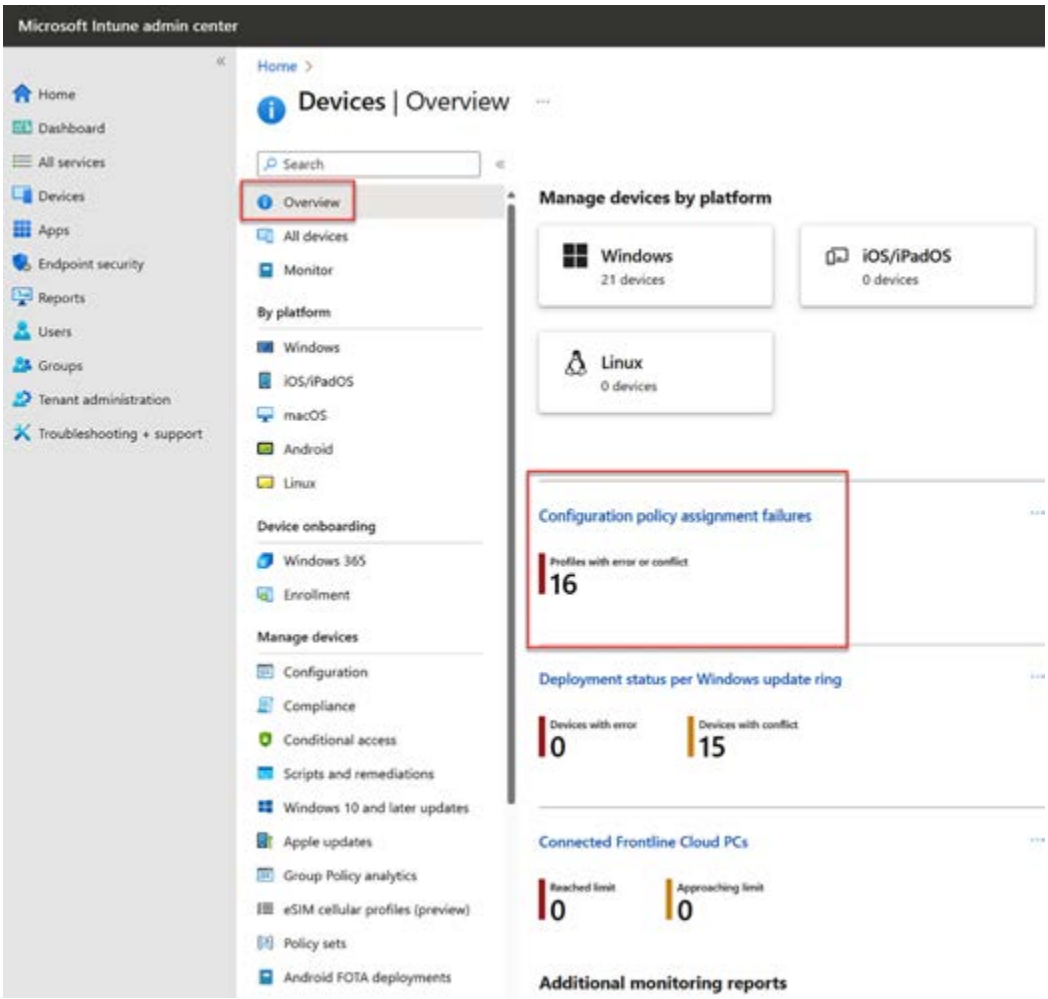


Figure 9.14: Configuration policy status

2. You can see the policy that has conflicts and the work required to remediate the conflict:

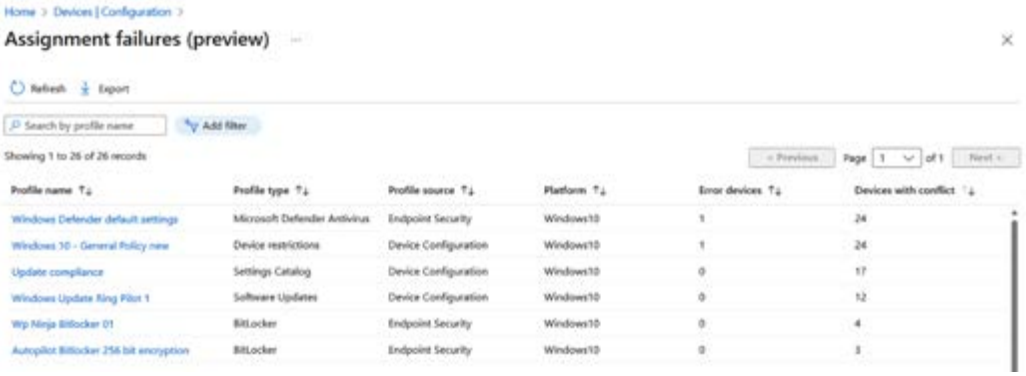


Figure 9.15: Policy conflict

3. When drilling down into the policy, you can see which settings are in conflict. In this case, I see that there is a conflict between a policy in the **Endpoint Security** blade and the Antivirus – Windows Defender Antivirus policy type:

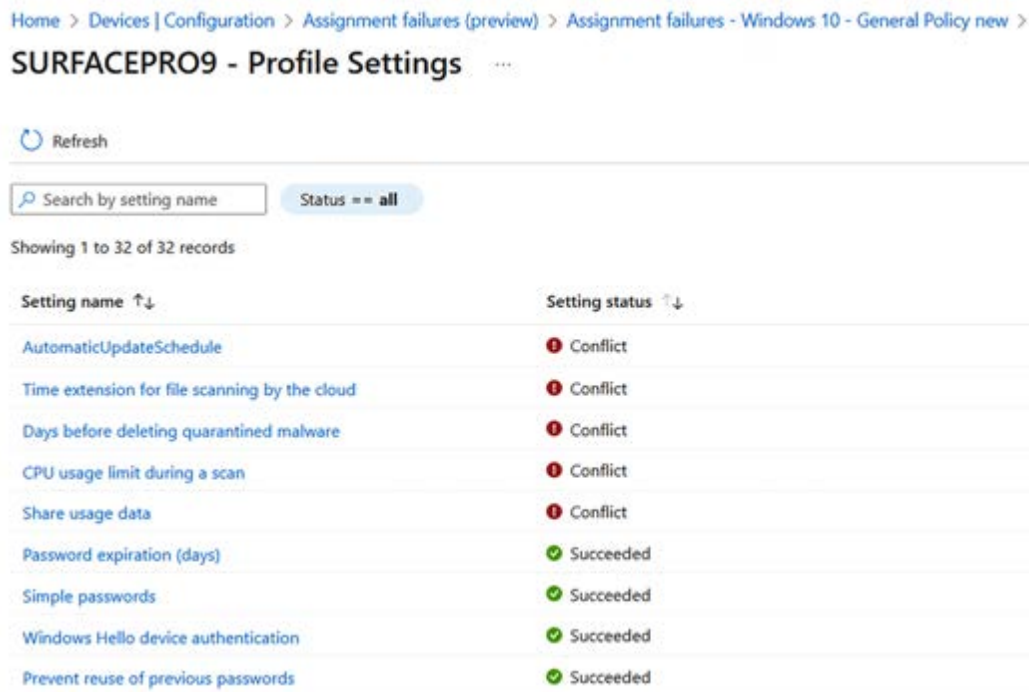


Figure 9.16: Profile settings

4. Going to that policy, you can see in the **Per-setting status** blade that the top line, **CPU usage limit per scan**, has conflicts. When you find conflicts, you need to go into the policies with conflicts and change the conflicting settings so they are only configured in one policy:



Figure 9.17: Per-setting status

Let's now have a look at how to implement different policy types.

Migrating existing policies from AD – Group Policy management

It's possible to migrate your existing Active Directory-based group policies into Microsoft Intune. This can be done with the Group Policy analytics feature.

Many businesses that are looking at Microsoft Intune management need a good path to the new modern workplace. The translation of existing policy settings to Intune can be tricky. This service will make life much easier for IT admins. Let me explain in more detail what Group Policy analytics does and how you can use it yourself; it can be found on the **Devices** blade:

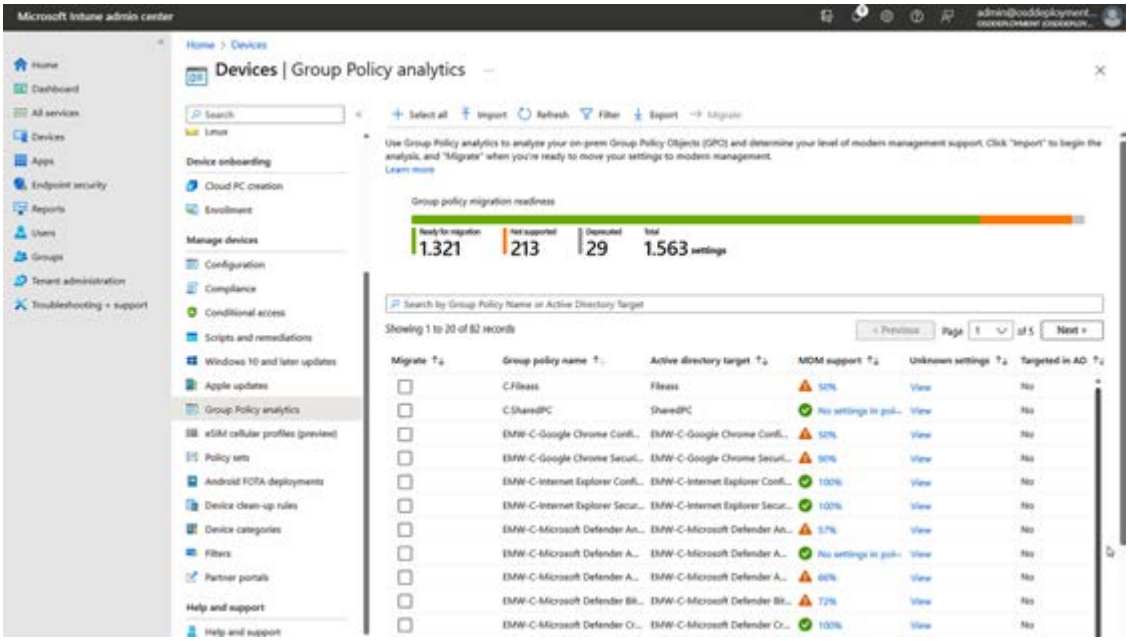


Figure 9.18: Group Policy analytics

1. First, make sure to perform an export of your existing policy settings from within your on-premises Group Policy Management console.
2. Export the policies by right-clicking and selecting **Save Report...**.

3. Save the files somewhere centralized, as we need to upload them to Microsoft Intune:

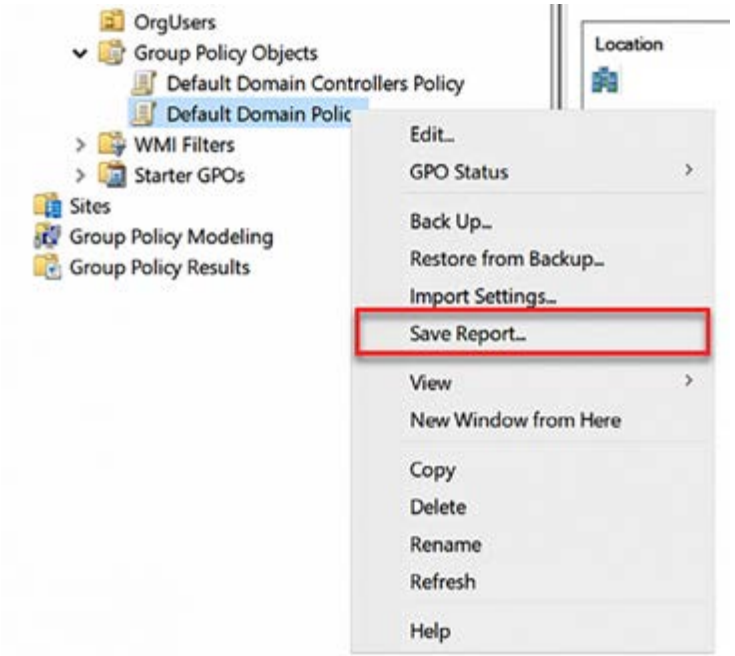


Figure 9.19: Save the policy report

4. In the Microsoft Intune admin center, select **Devices** | **Group Policy analytics**.
5. Click on **Import:**



Figure 9.20: Import

6. Search for the policy report file you exported:



Figure 9.21: Import the GPO files



NOTE

When you have multiple policies, you can upload them all here, too, for further analysis.

7. After you run the policy analysis, you will see the **MDM Support** column (which also applies to Windows), showing how many of your settings/policies are also available in Microsoft Intune to migrate from GPOs to Intune settings on a 1:1 basis:



Figure 9.22: MDM Support

8. You will get the information you need to proceed. The GPOs you imported are now all listed with the following information:

- **Group policy name**: The name is automatically generated using the information in the GPO.
- **Active Directory Target**: The target is automatically generated using the **Organizational Unit** (**OU**) target information in the GPO.
- **MDM Support**: This shows the percentage of Group Policy settings in the GPO that have the same setting in Intune.
- **Targeted in AD**: **Yes** means the GPO is linked to an OU in an on-premises Group Policy. **No** means the GPO isn't linked to an on-premises OU.

- **Last imported:** This shows the date of the last import.

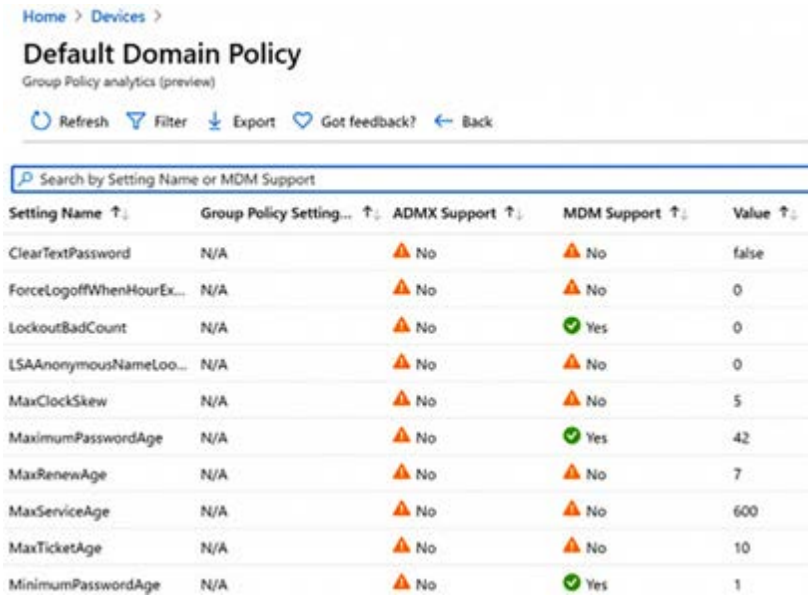


Figure 9.23: Default Domain Policy

With Group Policy analytics, you import your on-premises GPOs. The tool analyzes your imported GPOs and shows the settings that are also available in Microsoft Intune. For the settings that are available, you can create a Settings Catalog policy and then deploy the policy to your managed devices.

9. After you have imported your GPOs, you can select the GPO that you want to migrate to Intune by clicking the **Migrate** button.

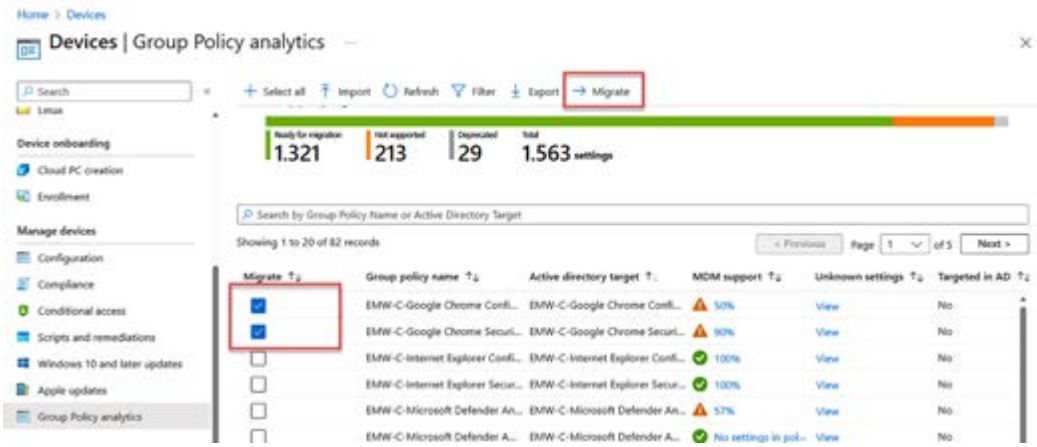


Figure 9.24: Migrating GPOs to Intune

10. You need to select the GPO settings that you want to migrate and then click **Next:**

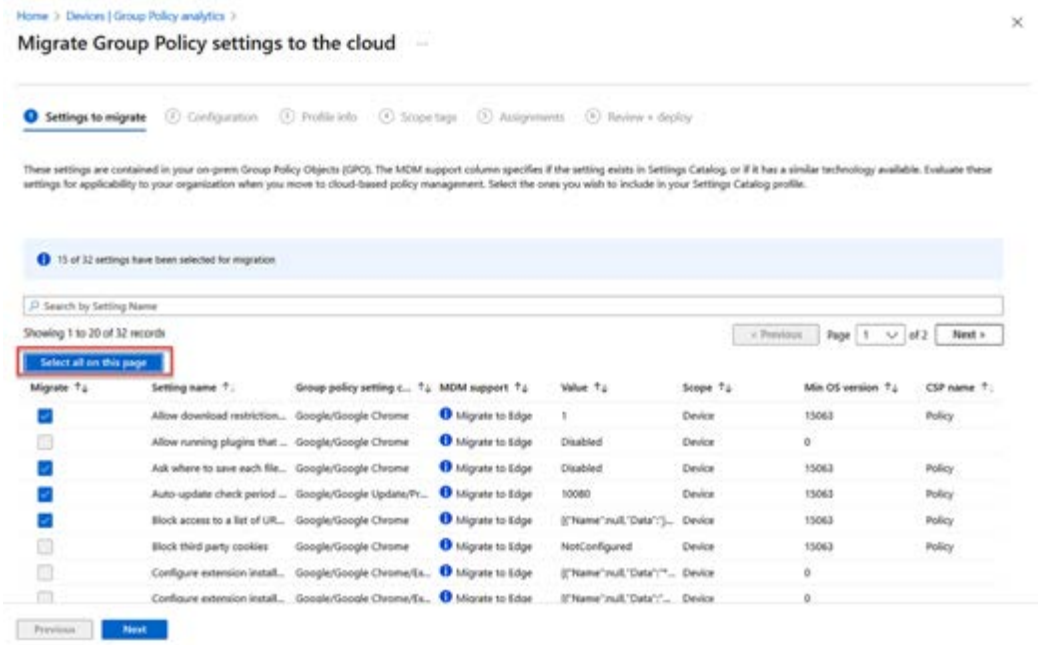


Figure 9.25: Migrating GPOs to the cloud

These are the settings you've identified as necessary to your organization as you move to cloud-based policy management. Configure the setting values as per your organization's requirements. Where possible, we configured the settings values as per the Group Policy:

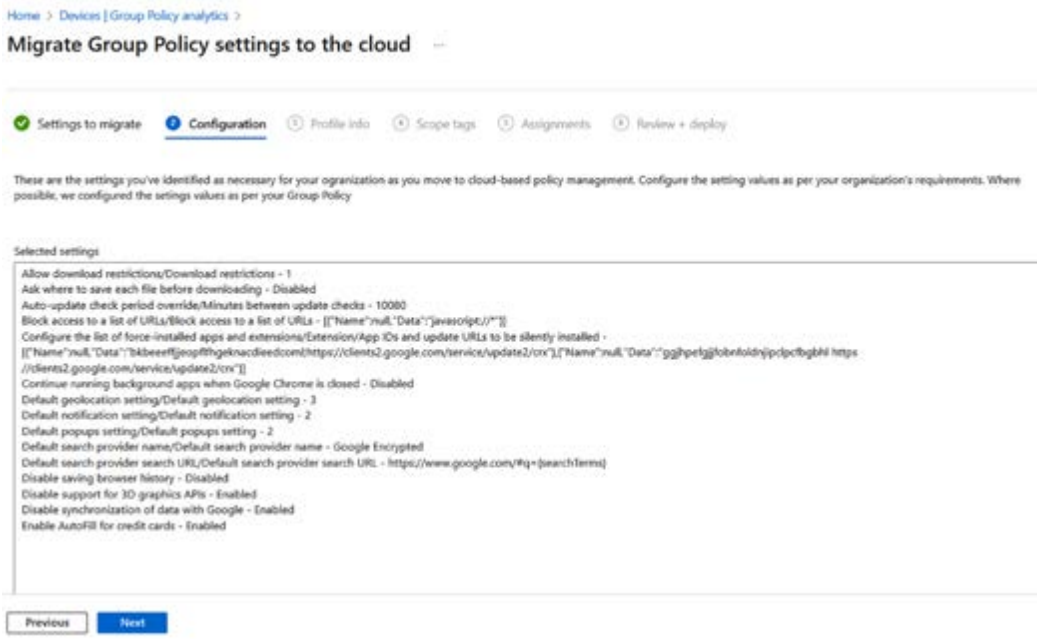


Figure 9.26: Migrating GPO settings

11. You need to give the new settings catalog profile a name:

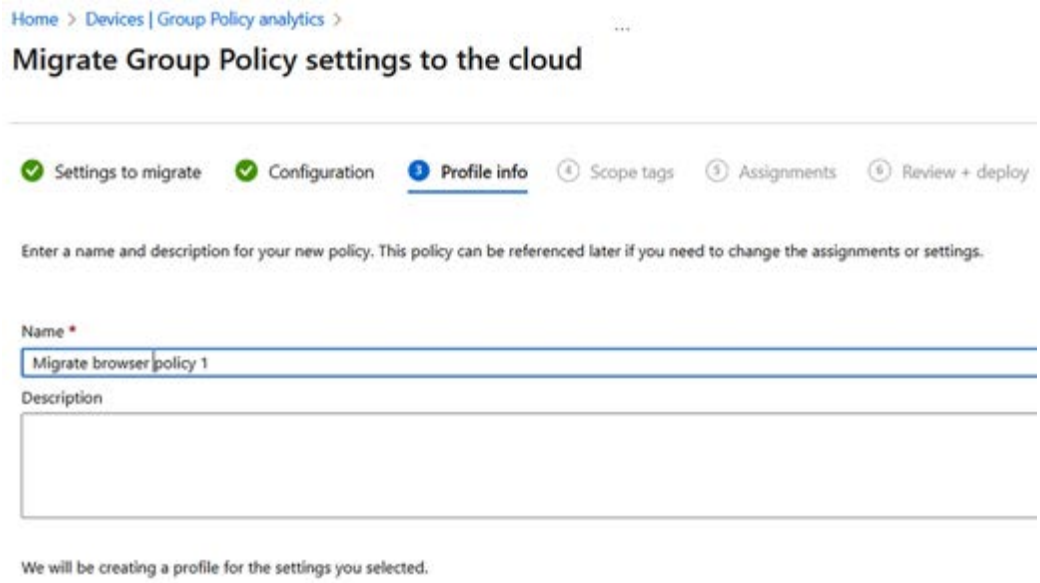


Figure 9.27: Migrating profile info

12. Continue with the guide to add scope tags and assignments, and then finally deploy the policy. You can skip the assignment and the policy will be created without an active assignment.

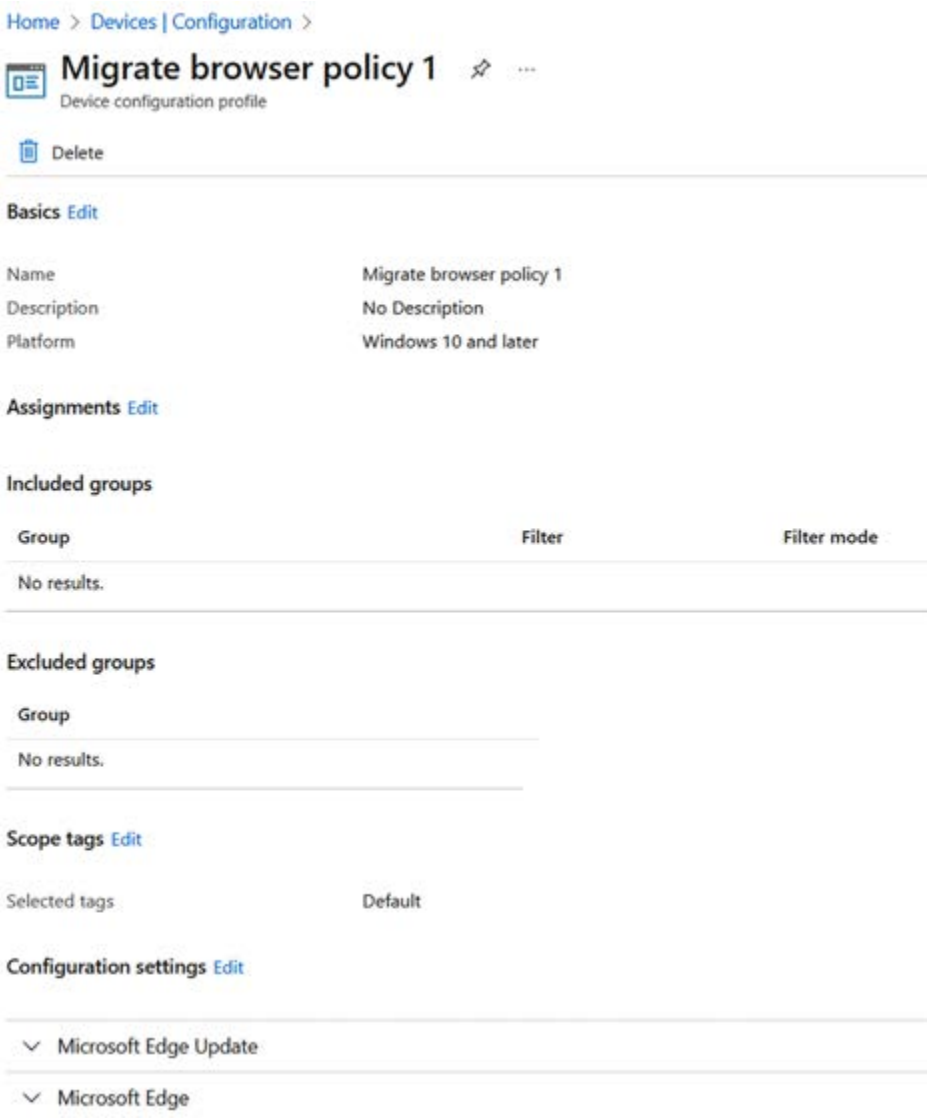


Figure 9.28: New browser policy

You have successfully migrated your browser policy and are ready to test it on Intune-managed devices before you deploy the policy at scale.

This concludes the section on Group Policy analytics, which can help you with your policy migration from on-premises GPOs to Microsoft Intune MDM policies.

Summary

In this chapter, you've learned about the basic policies in Microsoft Intune and how they apply to your Windows endpoints. This is knowledge that you can use to better understand what happens on a Windows device when you start to deploy policies to your endpoints from Microsoft Intune.

In the next chapter, we will go into more depth on how to configure different policy types from within Microsoft Intune.

Questions

1. Do CSP and ADMX policies write to the local registry in the same way?
    a. No
    b. Yes
2. What is the maximum number of devices for bulk actions in MDM?
    a. 10
    b. 50
    c. 100
    d. 1000
3. What does WNS stand for?
    a. Windows Name Server
    b. Windows Push Notification Service

Answers

1. (a)
2. (c)
3. (b)

Further reading

If you want to learn more after reading this chapter, please use the following free online resources:

- *Manage endpoint security in Microsoft Intune | Microsoft Docs*: `https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security`
- *Device compliance policies in Microsoft Intune – Azure | Microsoft Docs*: `https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started`
- *Use templates for Windows 10 devices in Microsoft Intune – Azure | Microsoft Docs*: `https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows`
- *Restrict device features using policy in Microsoft Intune – Azure | Microsoft Docs*: `https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-configure`

Get This Book's PDF Version and Exclusive Extras

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

Note: *Keep your invoice handy. Purchases made directly from Packt don't require one.*

UNLOCK NOW



10

Advanced Policy Management

This is the second chapter on policy management in this book. You will learn about the different policy options available to customize and secure the Windows 10 and Windows 11 Enterprise desktops in your environment. This chapter will be very broad in terms of content and topics related to Windows OS customizations, Microsoft 365 apps (Office, OneDrive, and so on), and Group Policy management.

We will cover different scenarios – some partial scenarios and some end-to-end scenarios. The most important part of this chapter is about the different policy options that exist in Microsoft Intune, and when and how you can leverage the different policy types in the best way to accomplish the task you need for your enterprise.

In this chapter, we'll be covering the following topics:

- Configuring a policy from the Microsoft Intune **Security** blade
- Configuring your Endpoint security profile
- Windows unhealthy endpoints
- Configuring a policy from the Settings catalog
- Configuring administrative templates
- OneDrive Known Folder Move configuration
- OneDrive – block syncing specific file extensions
- Configuring device configuration (template)
- Leveraging a custom policy as the last resort
- Pushing PowerShell scripts – scripted actions to endpoints
- Compliance policies
- Organizational compliance report

Policy management

Using Microsoft Intune to manage your Windows 10 or 11 Enterprise desktops is all about standardizing and simplifying the management layer of your environment. In *Chapter 9*, *Understanding Policy Management*, we covered the basics of how MDM policies work on the client side. We also learned how to get started with MDM policy management either from scratch or with Group Policy analytics.

In this chapter, we will look at different ways to configure settings within Microsoft Intune. We will start with security baselines as those are best practices for securing your desktops.

Configuring a policy from the Microsoft Intune Security blade

You should start with a security baseline if your organization is ready for it. Let's say that your organization is already leveraging a Microsoft security baseline such as **Center for Internet Security** (**CIS**) Benchmarks. With GPOs today, you already know the impact that a security baseline can have on your Windows production environment. There are multiple different baselines in Microsoft Intune:

- **Windows Security Baseline**: Use the Windows Security baseline to help you secure and protect your users and devices. This baseline consists of recommendations for settings that impact security and is created by the Windows Security team. If you are already using some kind of security baseline in your **Group Policy Object** (**GPO**) today, it is highly recommended to adopt the Intune Windows 10 and Windows 11 Security baseline as well.
- **Microsoft Defender for Endpoint Baseline**: The Microsoft Defender for Endpoint baseline represents the default recommended configuration for Defender for Endpoint and might not match baseline defaults for other security baselines. This means that if you are leveraging this baseline in conjunction with the Windows 10 Security baseline, you can create conflicts between the different policy settings.
- **Windows 365 Security Baseline**: The Windows 365 Security baseline provides a set of policy templates built on security best practices and experience from real-world implementations. You can use security baselines to get security recommendations that can help lower risks. The Windows 365 baseline is one baseline for Cloud PC with security settings for Windows, Microsoft Edge, and Microsoft Defender for Endpoints. This also means that you should not assign other security baselines to the same group of devices as it can end up in a policy conflict.
- **Microsoft Edge Baseline**: The Microsoft Edge baseline sets the recommended configuration for the Microsoft Edge browser. The Microsoft Edge security baseline has a very small footprint and only sets security-related settings, so it is easy to test out in your organization. If you are allowing your users to use different browsers on company-owned Windows 10 devices, you should also create a security baseline on those third-party browsers; otherwise, there is a risk that your end users will always use the least secure browser.
- **Microsoft 365 Apps for Enterprise Security Baseline:** The security baseline for Microsoft 365 Apps for Enterprise is published twice a year, usually in June and December. This security baseline contains recommended security configurations for Microsoft 365 Apps for Enterprise.

Be aware that when a baseline changes its version, the old one will be read-only. You can continue to use those profiles, but you won't be able to edit them. You should change the baseline version to take advantage of the newest recommendations every time a new version is released.

The Microsoft Edge baseline defaults represent the recommended configuration for Microsoft Edge browsers, so they might not match the baseline defaults of other security baselines.

In this example, we are going to create a Microsoft Edge baseline policy:

1. Start by going to the Microsoft Intune admin center.
2. Select **endpoint security**.
3. Select **security baselines**.
4. Select **Security Baseline for Microsoft Edge**.
5. Click **Create Profile**.

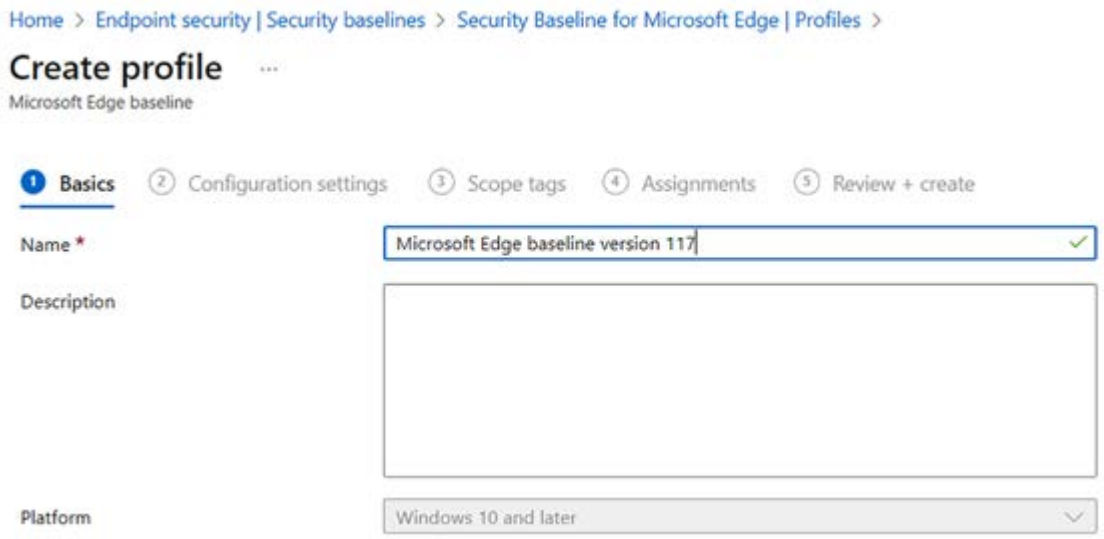


Figure 10.1: Microsoft Edge baseline – Create profile screen

You can change the settings within a security baseline if your tests have concluded that the settings in the baseline will not break apps or productivity in your environment. It is always recommended to deploy to a test group of users or devices before deploying a security baseline to the entire organization.

If you are happy with the settings, you can keep all the recommended values as is:

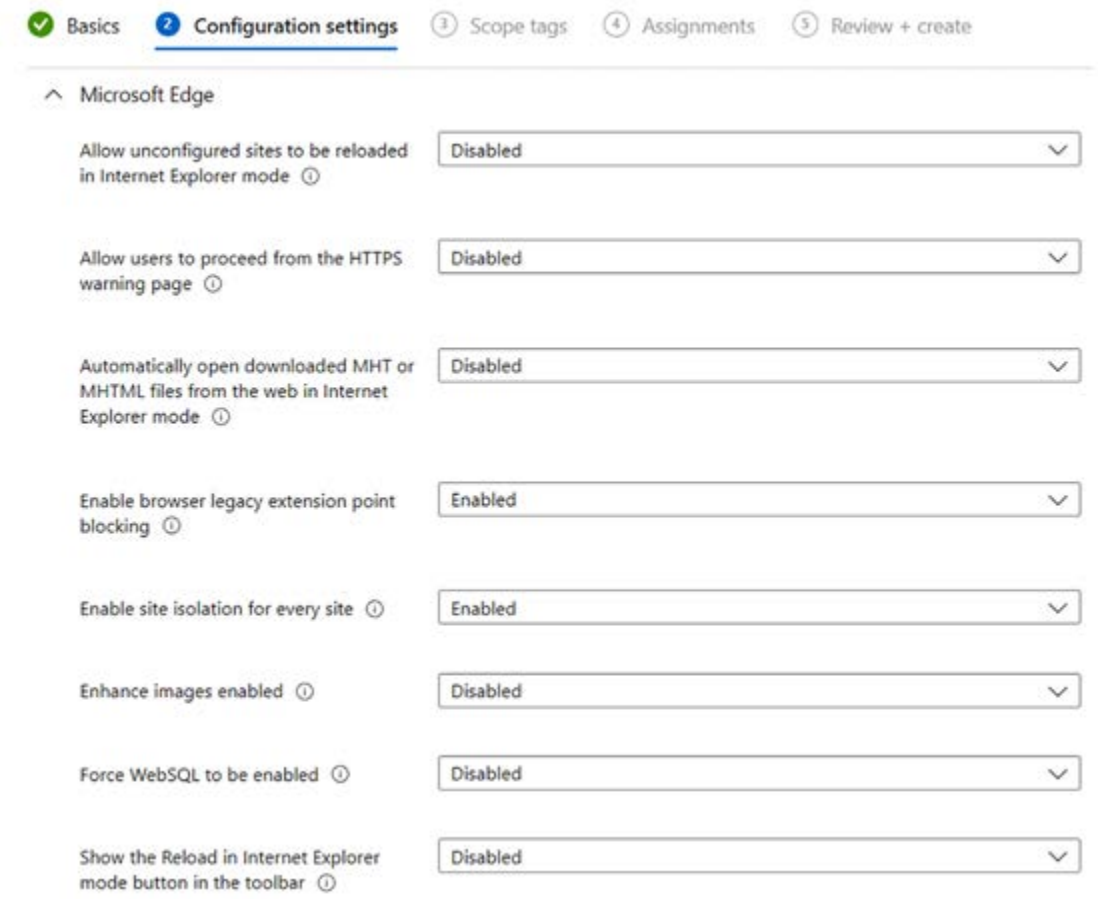


Figure 10.2: Microsoft Edge baseline – Configuration settings

Now you just need to assign the Edge security baseline to a group of users or devices. The Microsoft Edge security baseline is a set of preconfigured Windows settings designed to enhance security. These settings help organizations apply and enforce granular security measures recommended by relevant security teams. Here are some key points about the Edge security baseline:

Purpose and importance:

- The baseline ensures that Microsoft Edge, the web browser, adheres to security best practices.
- It helps protect against common threats, vulnerabilities, and attacks.
- By implementing the baseline, organizations can reduce risks and enhance their overall security posture.

Customization and enforcement:

- Organizations can customize the baseline to enforce only the settings and values they require.
- When creating a security baseline profile in Intune (Microsoft's unified endpoint management solution), administrators create a template consisting of multiple device configuration profiles.
- Each baseline version replaces the previous one, and older versions become read-only while still accessible.

This concludes this section on endpoint security baselines. Next, we will cover endpoint security policies.

Configuring your Endpoint Security profile

The **Endpoint security** node of Microsoft Intune was built to allow IT or security admins to configure device security. By using these security-focused policies, you will only see security-related policies in this blade view and not regular policies for other types of settings. Policies in the **Endpoint Security** blade can be applied to Windows, macOS, or Linux.

Here is the list of areas where you can configure policies in the **Endpoint Security** blade:

Antivirus – Antivirus is where you can configure different policies for Microsoft Defender, such as:

- **Defender Update controls**
- **Microsoft Defender Antivirus exclusions**
- **Microsoft Defender Antivirus**
- **Windows Security Experience**

Disk encryption – Endpoint security disk encryption profiles focus on only the settings that are relevant to a device's built-in encryption method, like FileVault or BitLocker. This focus makes it easy for security admins to manage disk encryption settings without having to navigate a host of unrelated settings:

- BitLocker
- Personal data encryption

Firewall – Use the endpoint security firewall policy in Intune to configure devices' built-in firewall for devices that run macOS and Windows 10/11:

- Windows Firewall Rules
- Windows Firewall
- Windows Hyper-V Firewall Rules

Endpoint detection and response – When you integrate Microsoft Defender for Endpoint with Intune, use the endpoint security policies for **Endpoint Detection and Response** (**EDR**) to manage the EDR settings and onboard devices to Microsoft Defender for Endpoint:

- Endpoint detection and response

App Control for Business (Preview) – Manage approved apps for Windows devices with App Control for Business policies and Managed Installers for Microsoft Intune. Intune App Control for Business policies are an implementation of **Windows Defender Application Control** (**WDAC**):

- App Control for Business

Attack surface reduction – When Defender Antivirus is in use on your Windows 10/11 devices, use Intune endpoint security policies for attack surface reduction to manage those settings for your devices:

- Attack surface reduction rules
- Device control rules
- Device control
- Exploit protection

Account protection – Account protection policies help you protect the identity and accounts of your users. The account protection policy is focused on settings for Windows Hello and Credential Guard, which is part of Windows identity and access management:

- Local admin password solution (Windows LAPS)
- Local user group membership
- Account protection (Preview)

Microsoft Defender policy

Antivirus policies include the same settings as endpoint protection or device restriction profiles for device configuration policies.

However, those policy types include additional categories of settings that are unrelated to antivirus policies. While the Windows Defender policy types in the **Endpoint Security** blade only contain Windows Defender settings, you can see the four different policy types here:

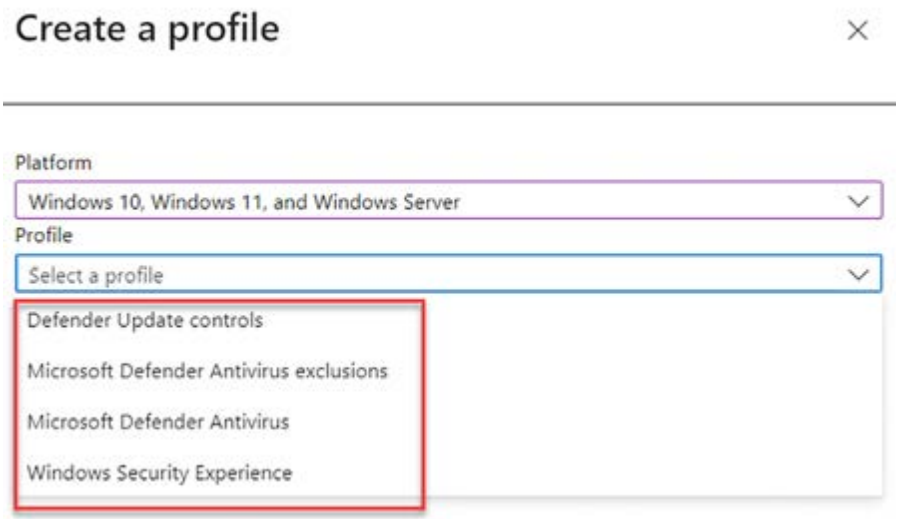


Figure 10.3: Windows Defender policy types

- Profile: **Defender Update controls**

  Configure the gradual release rollout of Defender Updates to targeted device groups. Use a ringed approach to test, validate, and roll out updates to devices through release channels. Updates available are platform, engine, and security intelligence updates. These policy types have pause, resume, and manual rollback commands similar to Windows Update ring policies.

- Profile: **Windows Security Experience**

  The Windows Security app is used by several Windows security features to provide notifications about the health and security of a machine. Security app notifications include firewalls, antivirus products, and Windows Defender SmartScreen.

  The **Windows Security Experience** profile can be used to turn off areas in the Windows Security app, such as **Family options** if you don't want to show family options on your Intune-managed devices:

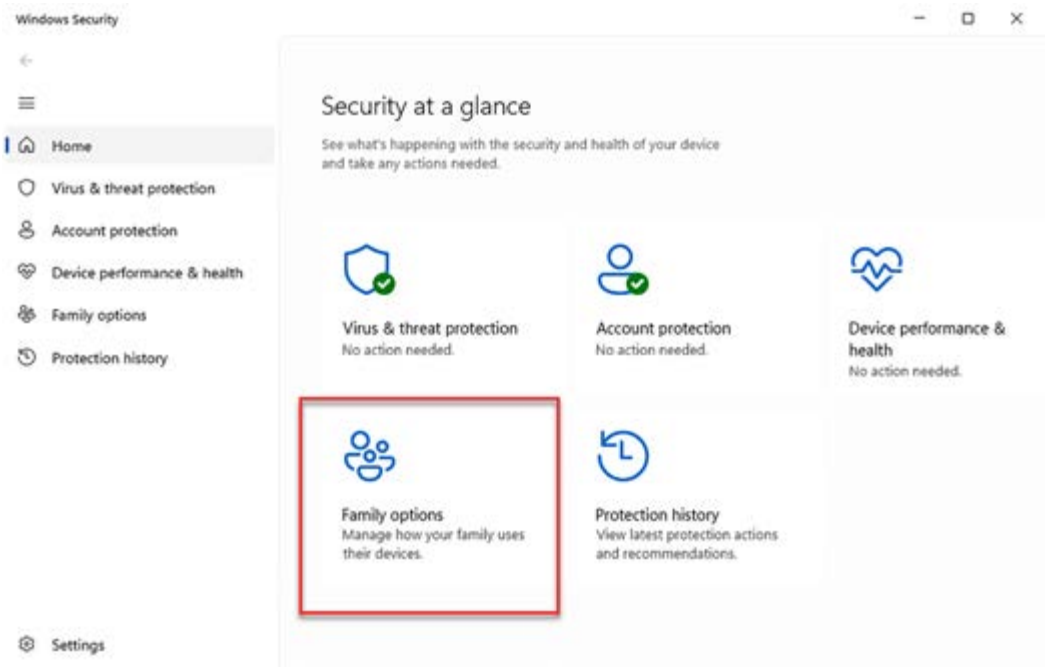


Figure 10.4: Windows Security app

- Profile: **Microsoft Defender Antivirus**

  Windows Defender Antivirus is the next-generation protection component of Microsoft Defender for Endpoint. Next-generation protection brings together machine learning, big-data analysis, in-depth threat resistance research, and cloud infrastructure to protect devices in your enterprise organization.

- Profile: **Microsoft Defender Antivirus exclusions**

  This template allows you to manage settings for Microsoft Defender Antivirus that define Antivirus exclusions for paths, extensions, and processes. Antivirus exclusions are also managed by the Microsoft Defender Antivirus policy, which includes identical settings for exclusions. Settings from both templates (Antivirus and Antivirus exclusions) are subject to policy merging and creating a superset of exclusions for applicable devices and users. This concludes this section on Windows Defender policies. Next, we'll learn how to monitor Windows Defender in Microsoft Intune.

Antivirus reporting in Endpoint security

In the **Endpoint security** blade, you will also find antivirus reports displaying status details about your Endpoint security antivirus policies and devices:



Figure 10.5: Unhealthy endpoints

The **Summary** tab gives you an overview of the Windows Defender status of your devices so that you can dive deeper into the reports.

Unhealthy endpoints

The **Unhealthy endpoints** tab gives you an overview of devices that are unhealthy. Within this report, you can leverage the device actions that are related to Microsoft Defender for unhealthy endpoints. As an example, if you have devices that have **Antivirus** (**AV**) signatures that are out of date, you can invoke a remote action on the affected client devices. The devices will then start the process of updating Windows Defender signatures:

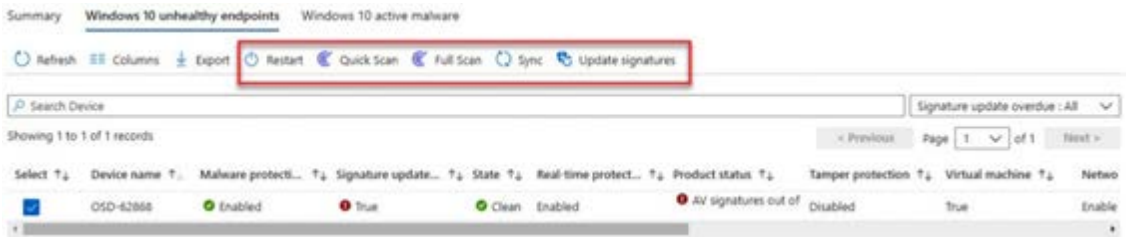


Figure 10.6: Unhealthy endpoints – remote action

This concludes our look at the basic Windows Defender AV settings. From a security perspective, you need to look at other security postures on devices as well. First, we will look at attack surface reduction, which is also part of the Windows Defender security stack on a Windows device.

Attack surface reduction

This is another important area with many different policy types that you can configure:

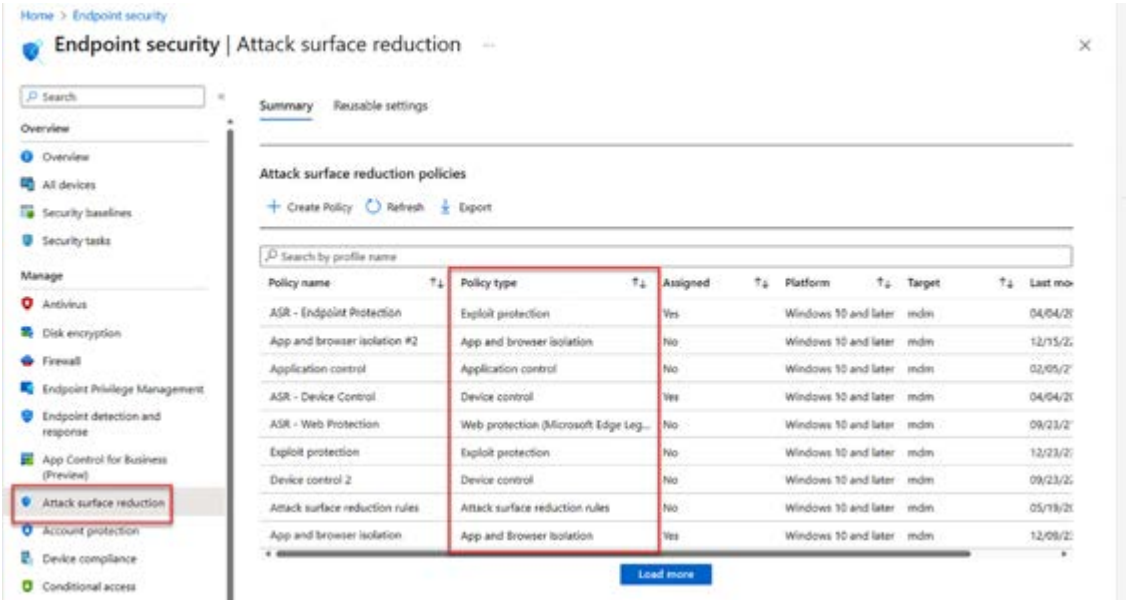


Figure 10.7: Attack surface reduction

A great example is the **Attack surface reduction rules** policy type.

Attack Surface Reduction (**ASR**) is a security feature in Windows that helps minimize the areas vulnerable to cyber threats and attacks. It achieves this by targeting specific software behaviors commonly exploited by malware and malicious apps.

ASR rules target behaviors that malware and malicious apps typically use to infect computers, such as executable files and scripts used in Office apps or webmail that attempt to download or run obfuscated files or otherwise suspicious scripts – behaviors that apps don't usually initiate during normal day-to-day work.

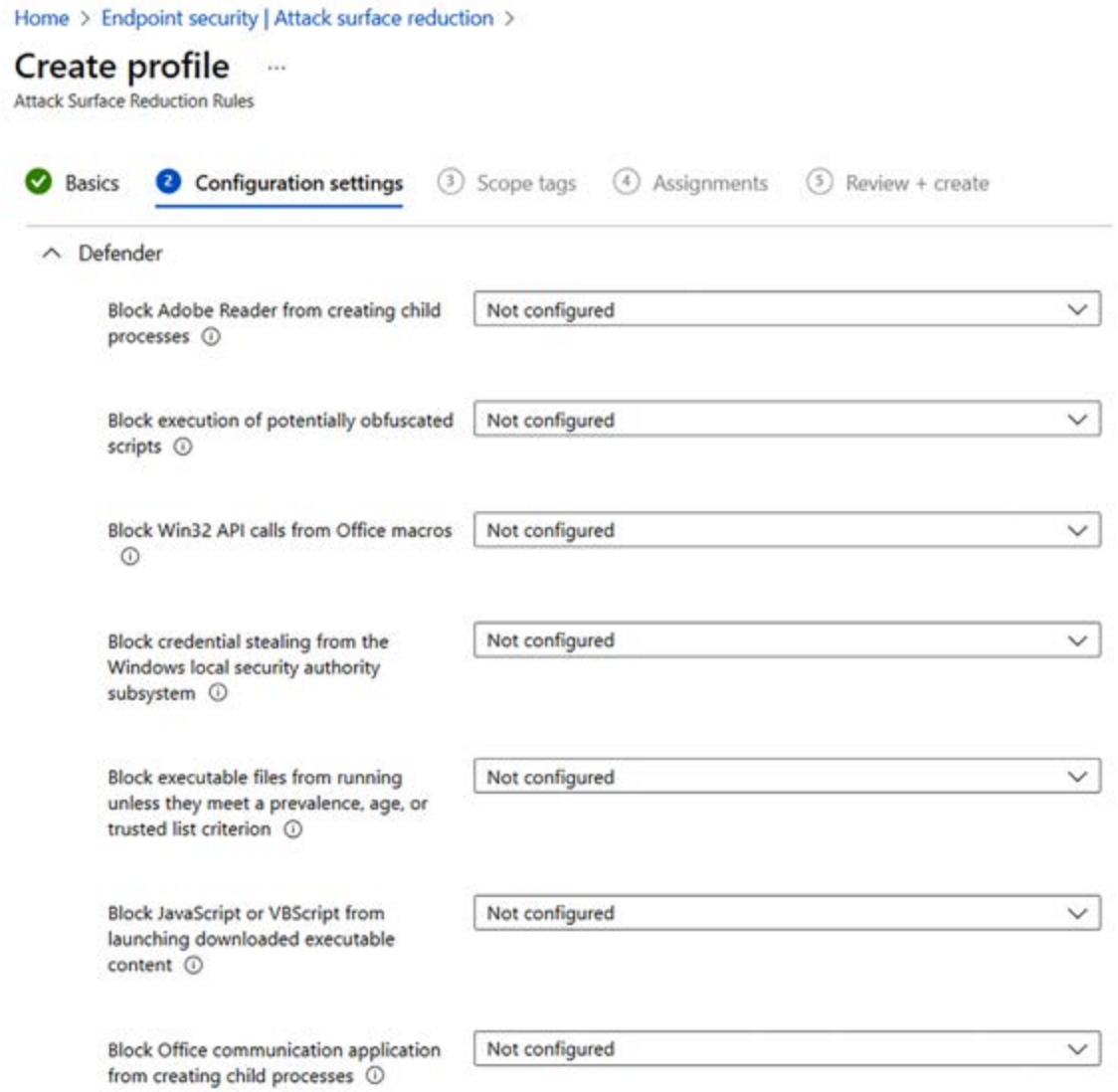


Figure 10.8: ASR rules

You can put the individual rules into different modes, where **Block** is the most restrictive one.

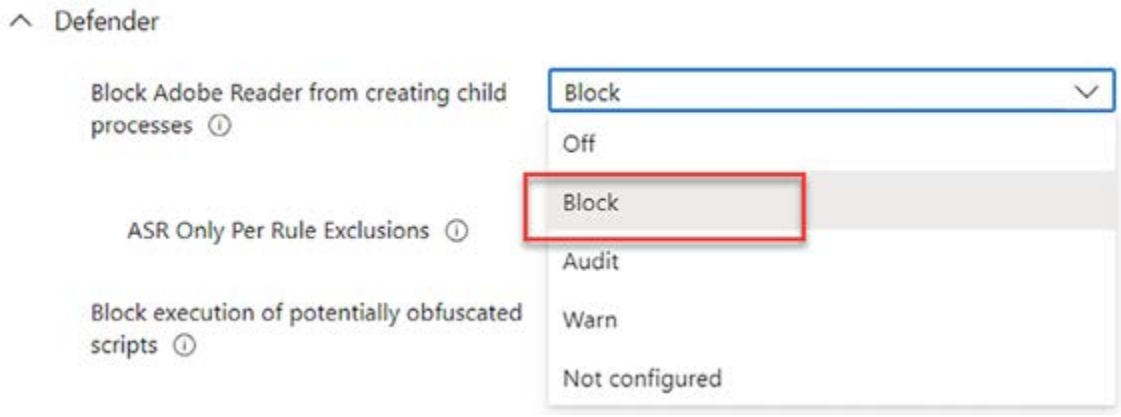


Figure 10.9: ASR block

Per rule exclusions:

- Exclusions can apply to all rules that allow them or they can be specific to certain rules.
- You can specify individual files, folder paths, or fully qualified domain names for resources.

Exclusions only apply when the excluded application or service starts.

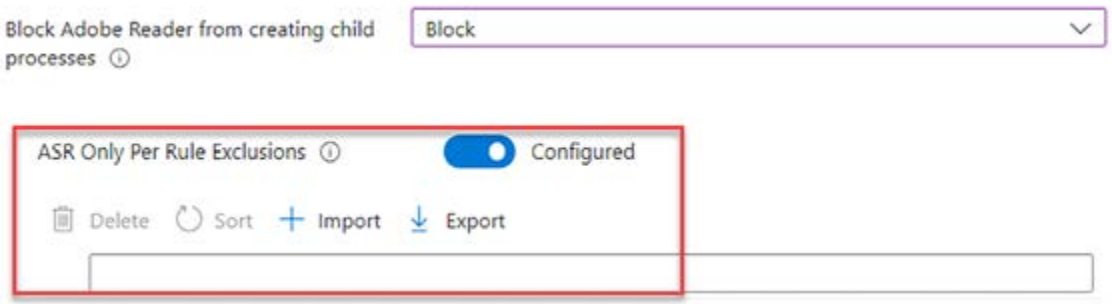


Figure 10.10: Per rule exclusions

When a device is assigned at least one policy that configures **ASR Only Exclusions**, the configured exclusions apply to all ASR rules that target that device. This occurs because devices receive a superset of ASR rule settings from all applicable policies, and the settings exclusions can't be managed for individual settings. To avoid having exclusions applied to all settings on a device, don't use this setting and instead configure **ASR Only Per Rule Exclusions** for individual settings.

Configuring a policy from the Settings catalog

The Settings catalog in Intune is a powerful feature that allows you to configure thousands of settings for Windows 10/11, iOS/iPadOS, and macOS client devices. Whether you're securing devices or controlling specific programs and features, the settings catalog simplifies the process. Here's what you need to know:

Windows platform-specific settings:

Windows 10/11: The settings catalog includes thousands of settings, some of which were previously unavailable. These settings are directly generated from the Windows **configuration service providers** (**CSPs**).

You can also configure Administrative Templates, with an expanded range of Administrative templates settings available.



Figure 10.11: Simplified policy creation workflow

When you create a new policy from the **Settings** catalog, no settings are configured initially, and the policy only contains the settings you specify. You have the option to remove one or more settings from a category with the settings picker.

The settings picker will allow you to search or browse to select any settings available in the settings catalog for configuration in your policy, and even allows you to add filters to search for a specific OS edition such as HoloLens, IoT Enterprise, or Windows Professional:

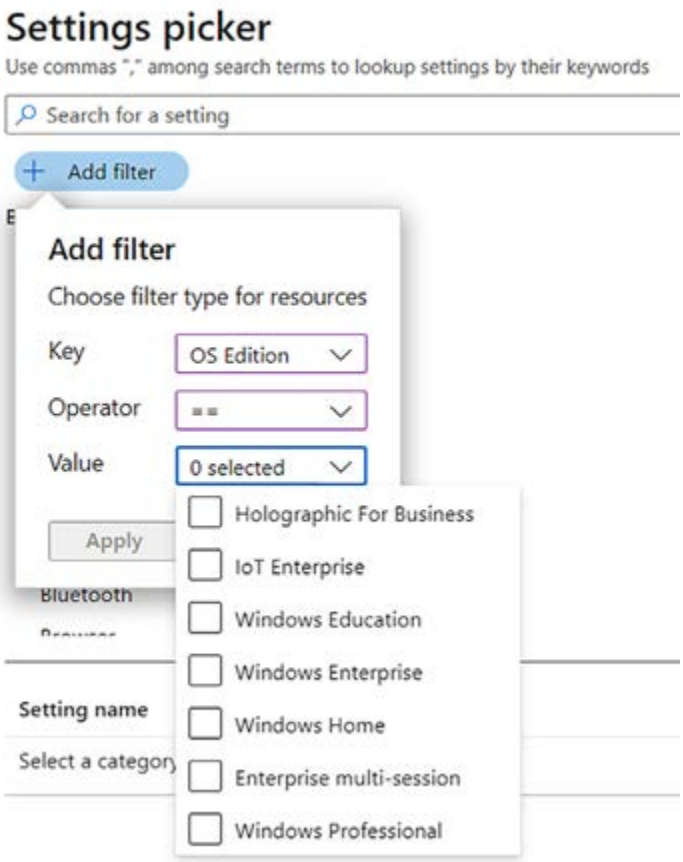


Figure 10.12: Settings picker – Add filter

The settings in the settings catalog are generated directly from Windows CSPs, and the settings experience in the catalog is dynamically generated based on the type of setting and its metadata, such as tooltips. The settings catalog continues to add new Windows settings and reduces the need to deploy custom policies from Microsoft Intune (OMA-URI-based). One of the new things in the settings catalog is that if a setting is not in your policy, then it will be considered not configured. Editing a policy later on and removing a setting from an existing settings catalog policy will not only remove that setting from the policy but it will also remove the previously set enforcement from assigned devices on the next device check-in.

There are thousands of settings to choose from in the settings catalog, including settings that are not in any other policy type in Microsoft Intune and have not been available before in the console. You can also configure **administrative templates** in the settings catalog. As Windows adds or exposes more settings to MDM providers, these settings are quickly added to the Microsoft Intune settings catalog to be configured.

To create a profile with the settings catalog, you need to open the Microsoft Intune admin center:

1. Go to **Home** | **Devices** | **Windows** | **Configuration profiles** | **Create New policy** and apply the following:
    - **Platform**: Select **Windows 10 and later**
    - **Profile type**: Select **Settings catalog**

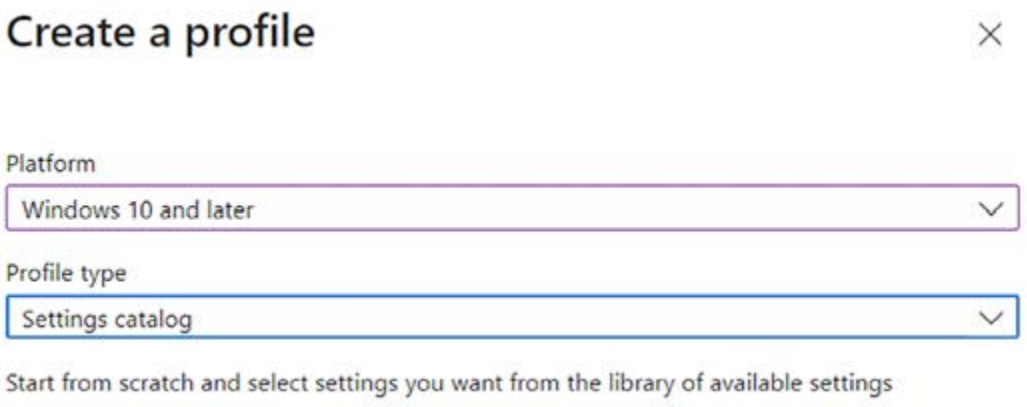


Figure 10.13: Create a profile

2. As part of the profile creation, you need to fill out the wizard:
    - **Name**: Enter a descriptive name for the profile, such as `Settings Catalog Policy`.

- **Description**: Enter a description for the profile. This setting is optional, but it is highly recommended to enter a description so that you can go back at a later point and see what the intent of this policy is:

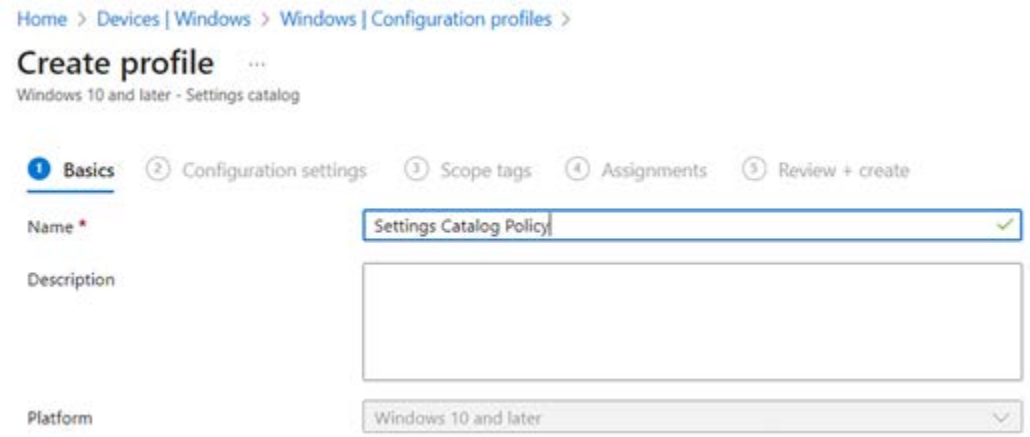


Figure 10.14: Create device configuration profile

3. In **Configuration settings**, select **Add settings**. In the **Settings picker**, select the **User Rights** category or another category to see all the available settings:

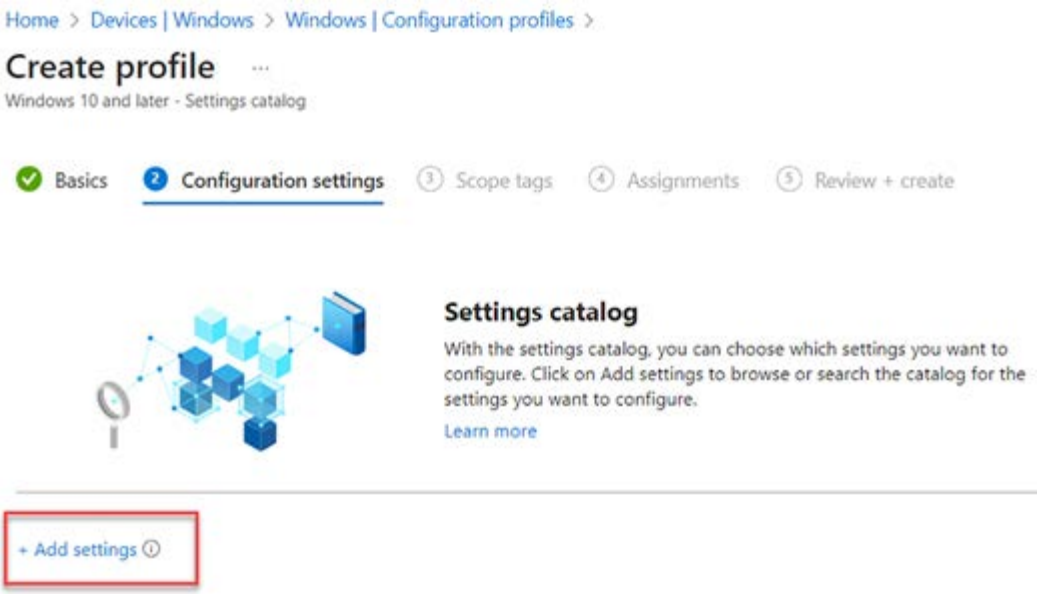


Figure 10.15: Create device configuration profile

4. The UI will automatically expand with the settings that you have just selected – in this case, the **User Rights** policy. Before the settings catalog was released, this was a policy where IT admins were forced to leverage a custom policy in Microsoft Intune, which required a lot of specialized knowledge:

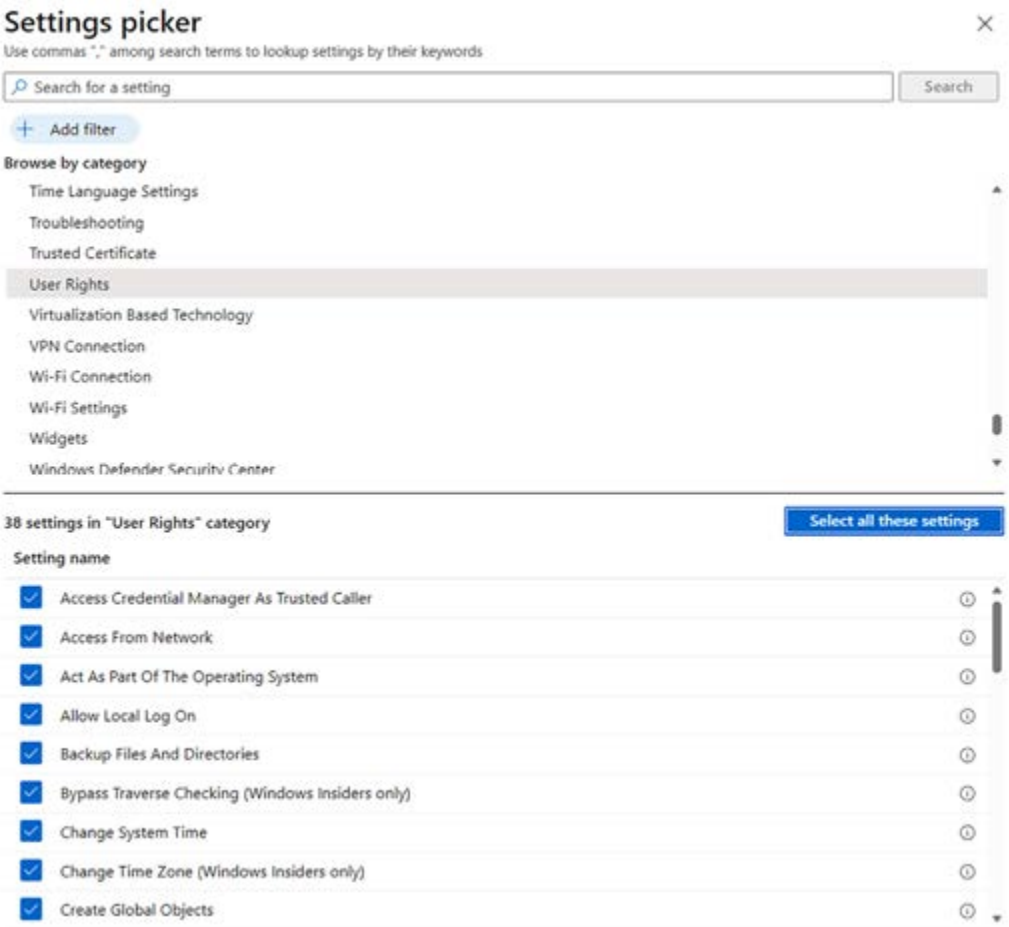


Figure 10.16: Settings picker



TIP

If you are not configuring all settings, you can remove individual settings by clicking the *not configured* icon, and the setting will be removed when saving the settings catalog. This means that it will not affect users or devices when deployed.

5. When configuring an individual setting, you can expand it with multiple values by clicking **Add settings:**

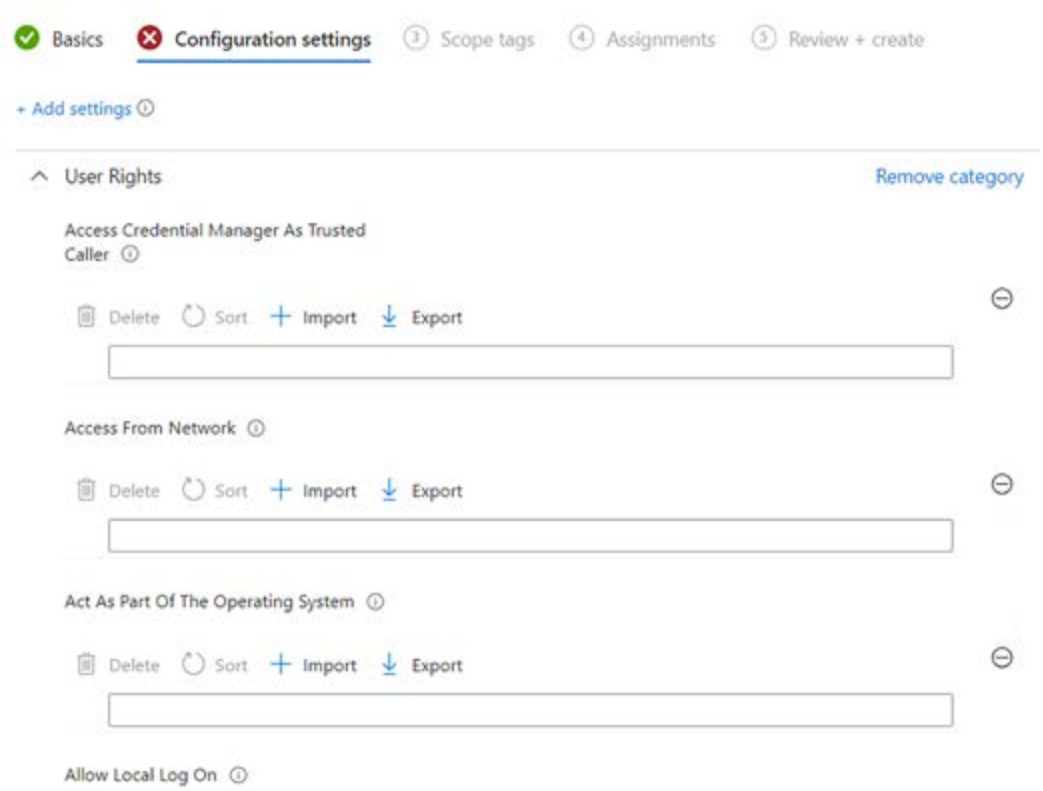


Figure 10.17: Create device configuration profile



TIP

The tooltip always gives you the required information on what the policy does. This is a part of the metadata from the **CSPs**. The tooltip also includes a **Learn more** link to the Microsoft Windows docs page for the underlying CSP.

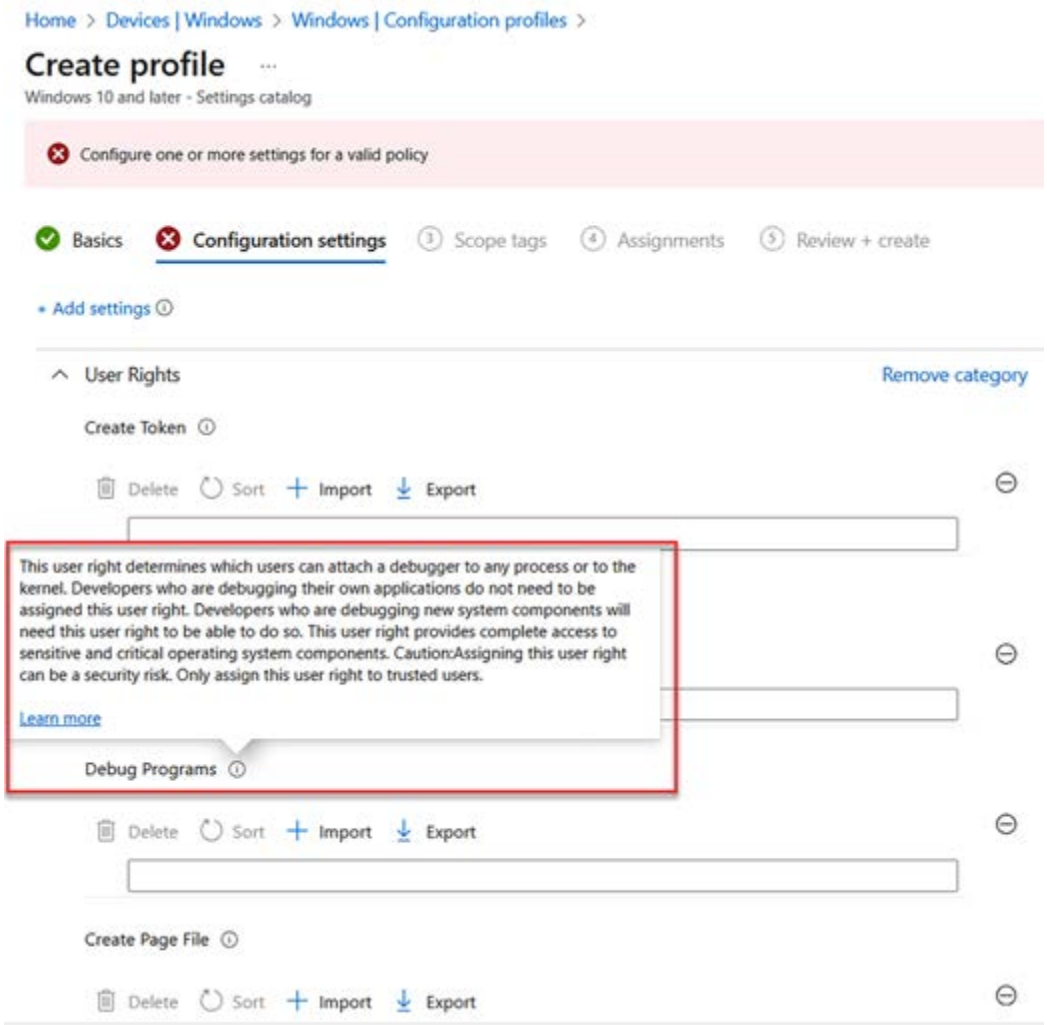


Figure 10.18: Settings picker tooltips

6. In this case, we are allowing users and administrators the right to local log on:



NOTE

This user right determines which users can log on to the computer. Modifying this setting may affect compatibility with clients, services, and applications. For compatibility information about this setting, see **Allow log on locally**: `https://go.microsoft.com/fwlink/?LinkId=24268`

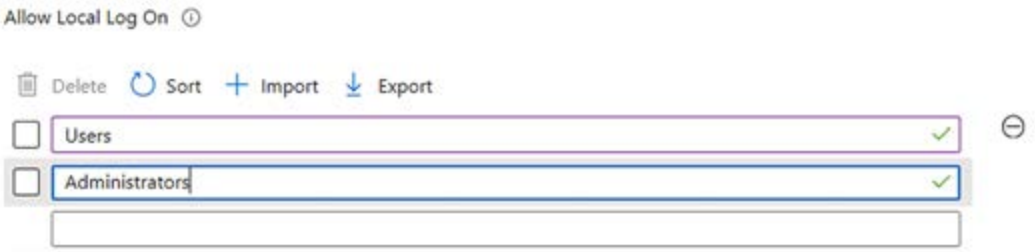


Figure 10.19: Allow Local Log On

7. You don't need a separator in the settings catalog, as you did in the past when creating the same policy as a custom policy in Microsoft Intune.

   In this case, we will also deny users with the Entra ID Global or Device Administrator roles from logging in to the devices. So, I will check the **security identifier** (**SID**) in the local administrator group on my Entra ID joined devices:



Figure 10.20: Deny Local Log On

You can also import or export the values in a CSV file.

8. From Windows 10 version 2004, you can leverage the SID for an Entra ID group:

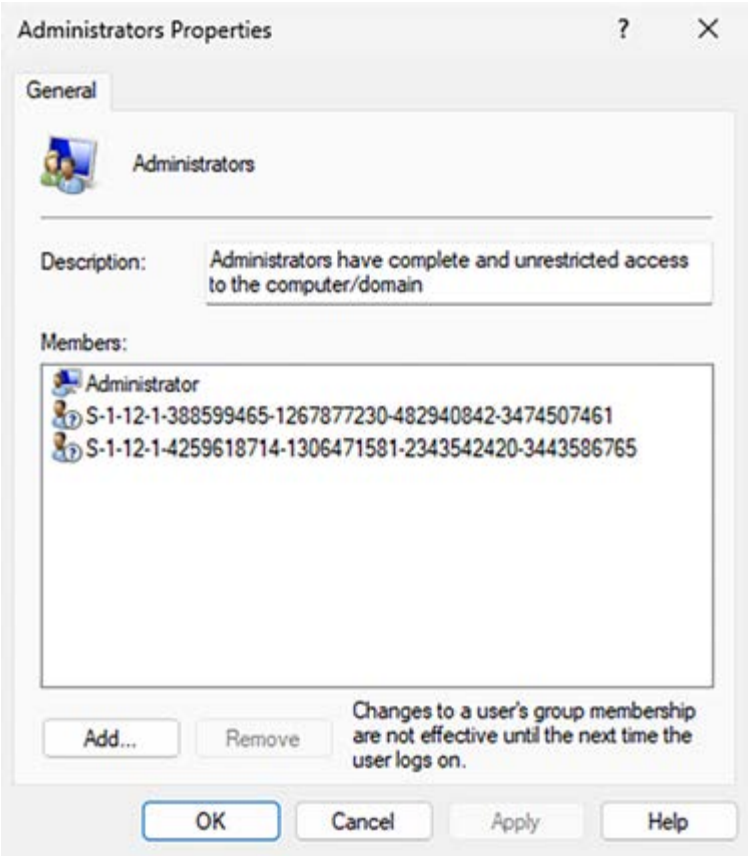


Figure 10.21: Administrators Properties

9. The SID can be found in the local administrator group on Windows 10 devices that are joined to your organization's Entra ID.

Each administrative template within an ADMX file specifies:

- The registry keys associated with a Group Policy.
- The values for those keys.
- The policy settings that can be managed.
- These templates can be edited using the Local Group Policy Editor on a PC.

What are ADMX files?

ADMX files are XML-based configuration files that define policy settings for Windows operating systems. They contain administrative policies related to user accounts, operating system configurations, and applications. Unlike traditional administrative templates, ADMX files offer a more convenient way to manage these settings.

The Settings catalog natively has **Administrative Template** (**ADMX**) support for the following ADMX templates:

- **Azure Virtual Desktop Terminal Server**: `https://learn.microsoft.com/en-us/azure/virtual-desktop/administrative-template?tabs=intune`
- **FSLogix**: `https://learn.microsoft.com/en-us/fslogix/how-to-use-group-policy-templates`
- **Google Chrome**: `https://chromeenterprise.google/policies/`
- **Microsoft 365 apps and Office**: `https://www.microsoft.com/en-us/download/details.aspx?id=49030`
- **Microsoft Edge**: `https://learn.microsoft.com/en-us/deployedge/microsoft-edge-policies`
- **OneDrive**: `https://learn.microsoft.com/en-us/sharepoint/use-group-policy#list-of-policies-by-string-id`
- **Visual Studio**: `https://learn.microsoft.com/en-us/visualstudio/install/administrative-templates?view=vs-2022`
- **Windows**: Built into the Windows client OS.
- **Windows Subsystem for Linux**: `https://learn.microsoft.com/en-us/windows/wsl/intune`

  Another example in the settings catalog is administrative templates for **Microsoft Edge Update**. The new Microsoft Edge is a Win32 app, so it leverages an ADMX policy instead of a CSP OMA-URI.

How do they work?

By browsing by category, you can find **Microsoft Edge Update:**

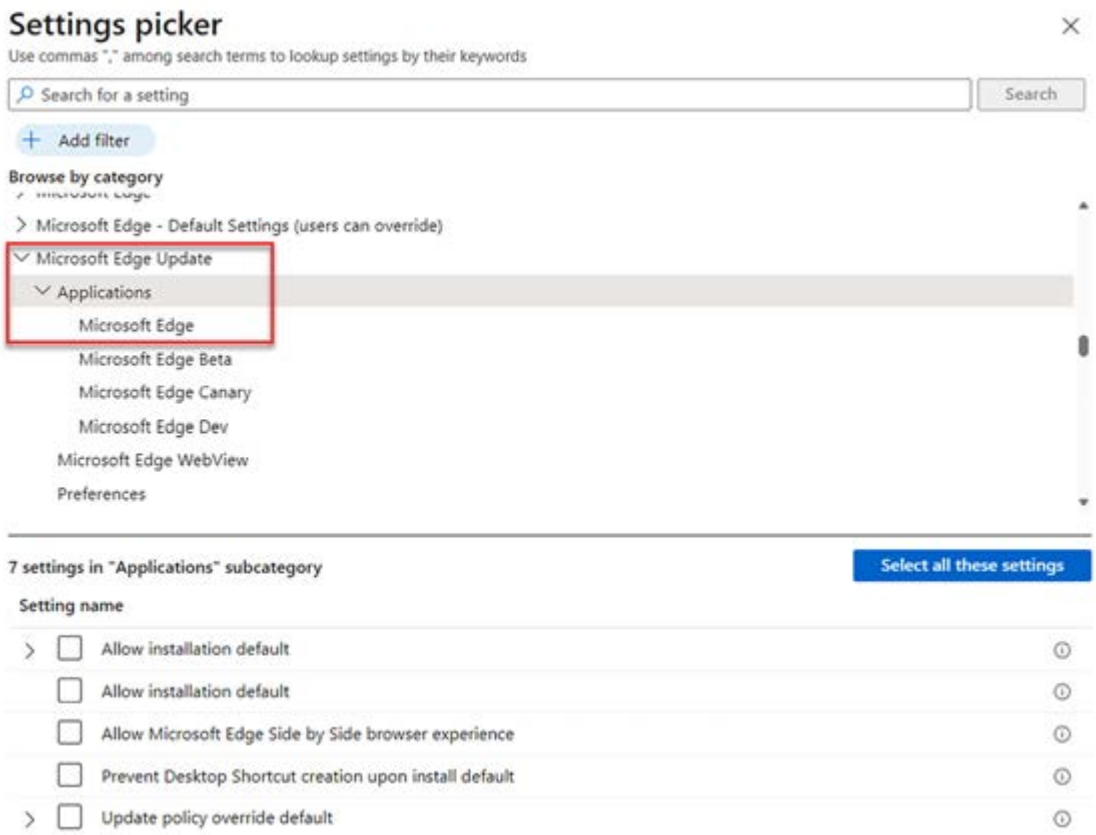


Figure 10.22: Settings picker – Browse by category

1. Find the policy category you want to configure and click **Select all these settings** or **Select one or more individual settings.** In this case, we will select **Microsoft Edge Update:**

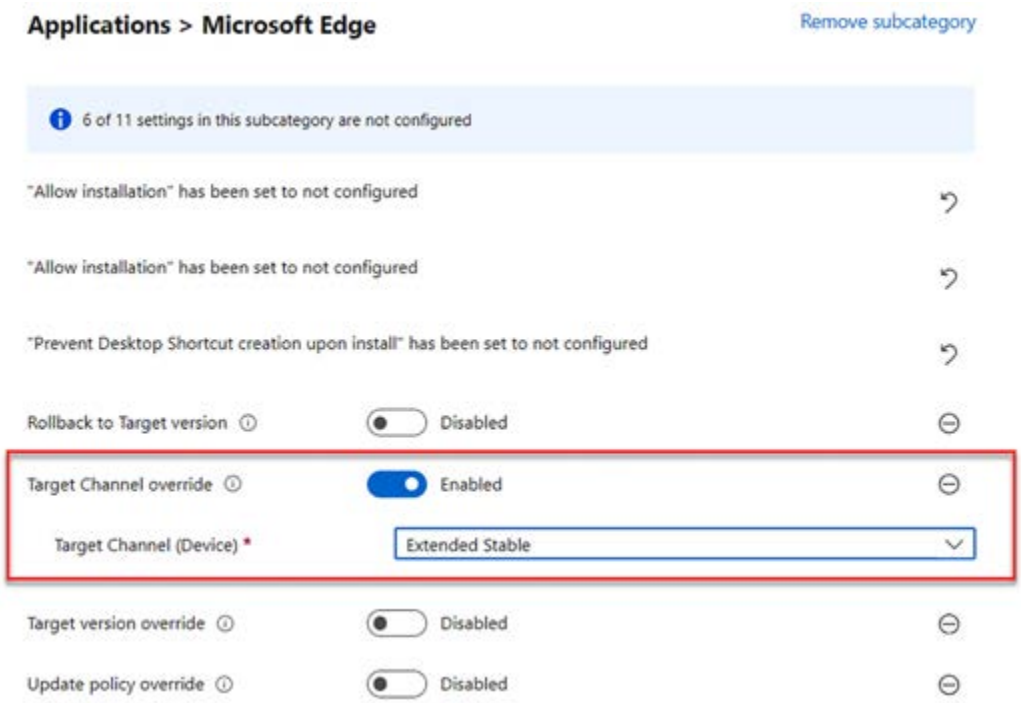


Figure 10.23: Edge Update configuration

2. Configure the settings you want to set and remove the ones you do not want to configure on your devices.

   In this case, we have configured the setting in **Applications | Microsoft Edge** called **Target Channel override**, with it set to **Enabled.** When we enable the setting, the UI dynamically expands and gives the option to configure **Target Channel (Device).** Certain settings have been removed, like **"Allow installation" has been set to not configured.** This means that the setting has been set to **Not configured.** This is a different behavior than some of the other profile types in Microsoft Intune, where settings are either **Enabled** or **Disabled.**

3. In **Applications** | **Microsoft Edge** | **Microsoft Edge Beta**, we have configured two settings and removed the rest:



NOTE

You, as an IT admin, can at a later point go in and re-add the category or subcategory again, if you need to configure the settings you just removed.

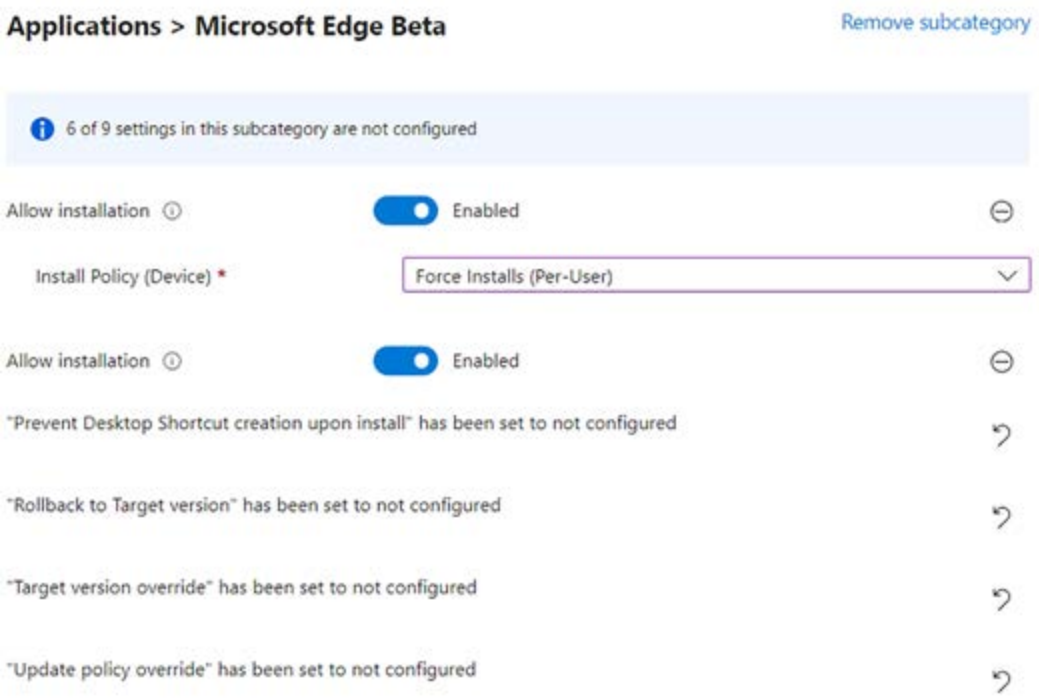


Figure 10.24: Settings in this subcategory are not configured

4. When we, at a later point in time, edit the settings catalog policy, we will only see the settings that we configured in the first place.

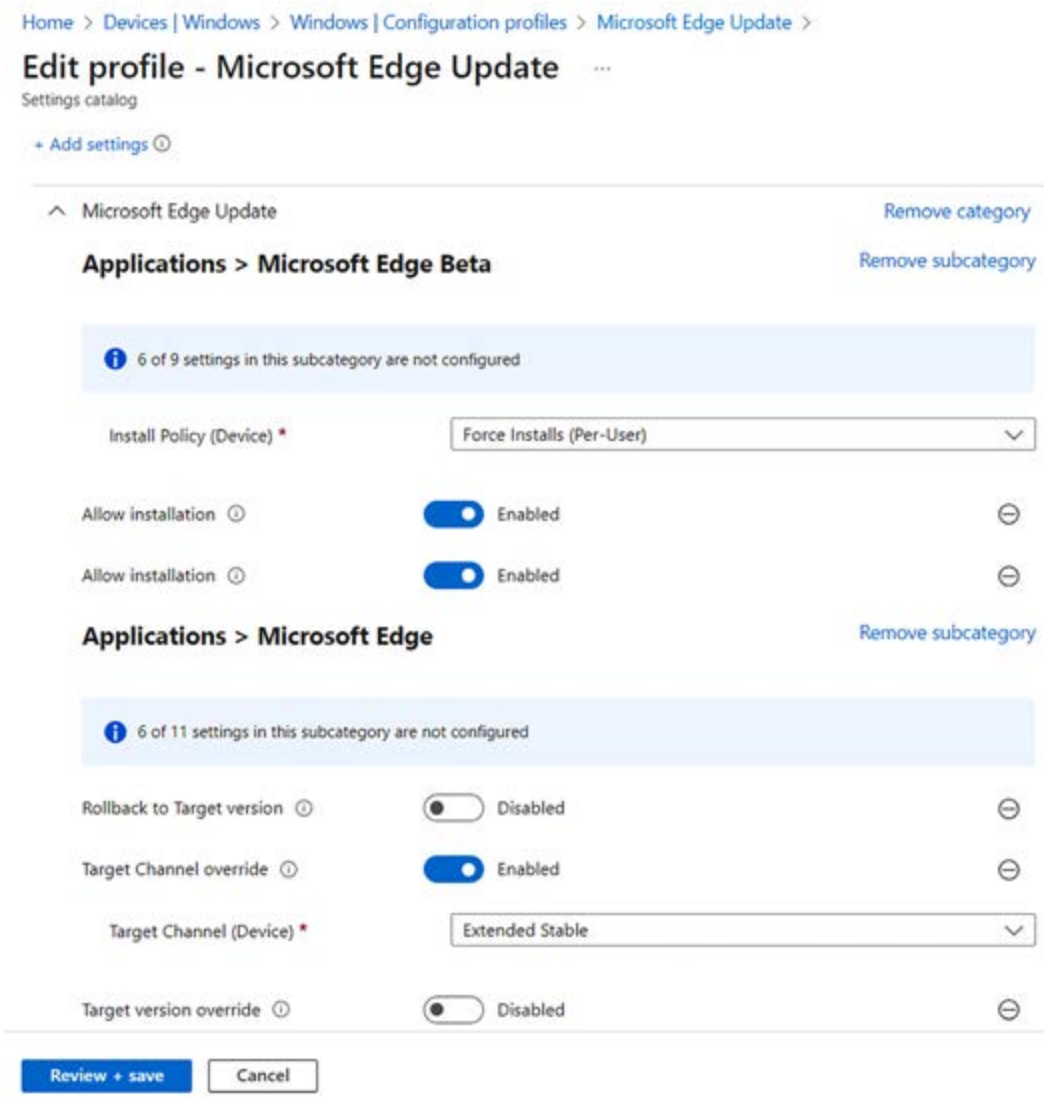


Figure 10.25: Settings catalog policy reopen

Settings catalog policies can also be both duplicated and exported as JSON. Duplicating creates a copy of the original policy with the specified name, allowing you to make adjustments or apply it to different groups as needed. Exporting gives you a backup of the policy that you can reimport at a later point, either in the same tenant or in a different tenant.

A great example is if you have an Intune tenant where you create and test all your policies, then you can export them and import them into your production tenant.

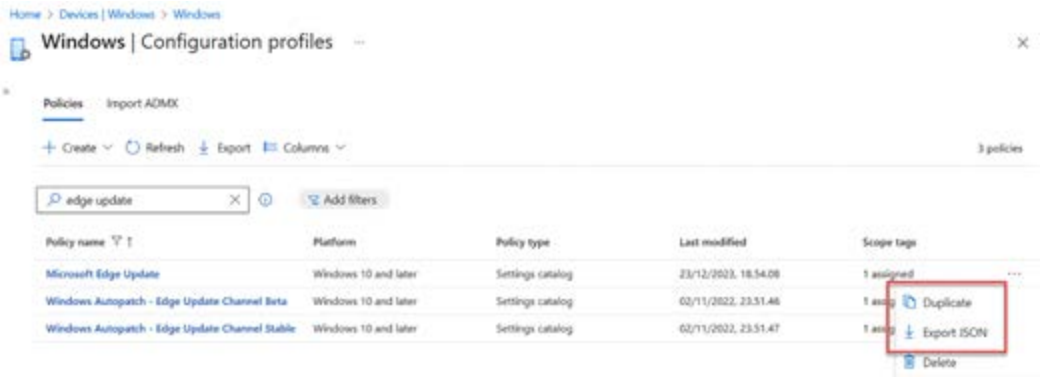


Figure 10.26: Settings catalog options

When you hit **Duplicate**, you get a new window where you have to enter a new name for the duplicated policy.

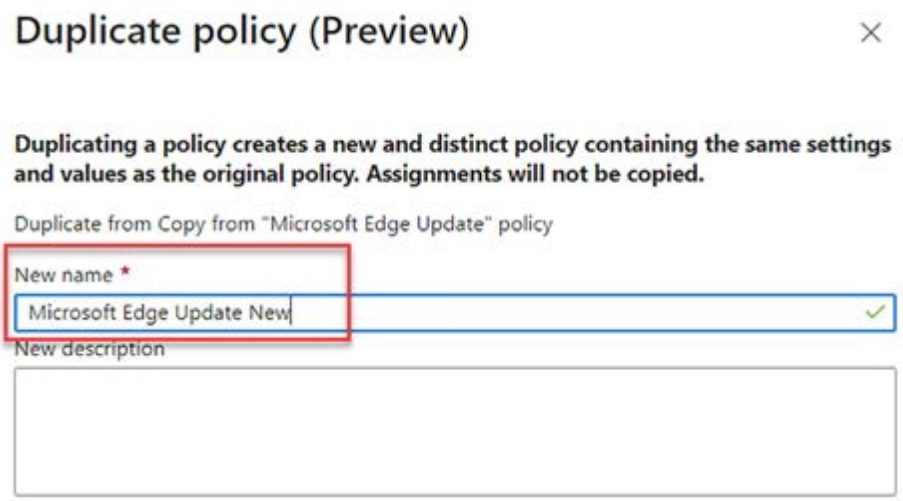


Figure 10.27: Settings catalog duplicate

If you instead hit **Export JSON**, you will get a **Download** button.

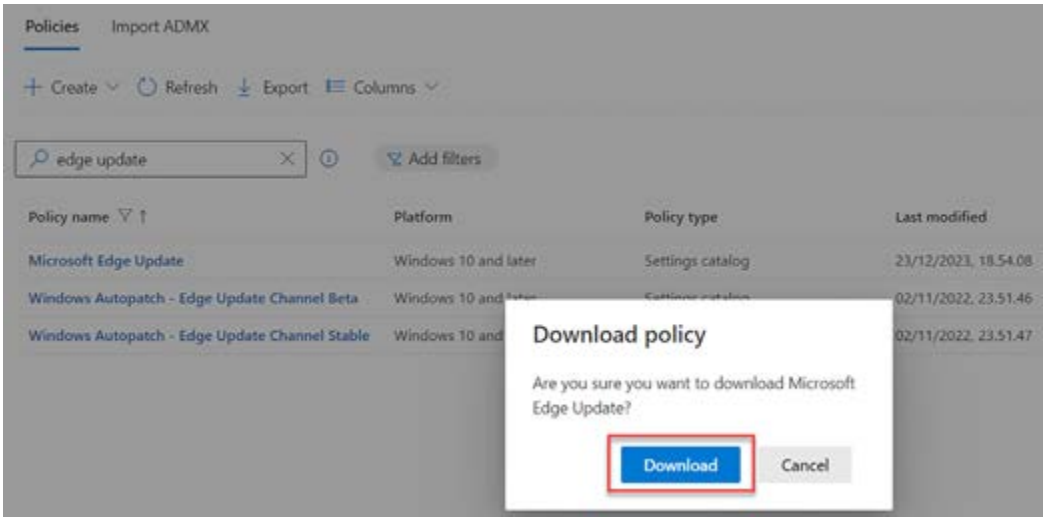


Figure 10.28: Settings catalog export JSON

Then you can change the JSON file and leverage Graph to import it again with the changed settings. You can even import it into a different tenant, for example, if you have a test tenant.

Create your policy and then just export it as JSON and leverage Graph or the native building import function in the Microsoft Intune admin center to import it into a new tenant.

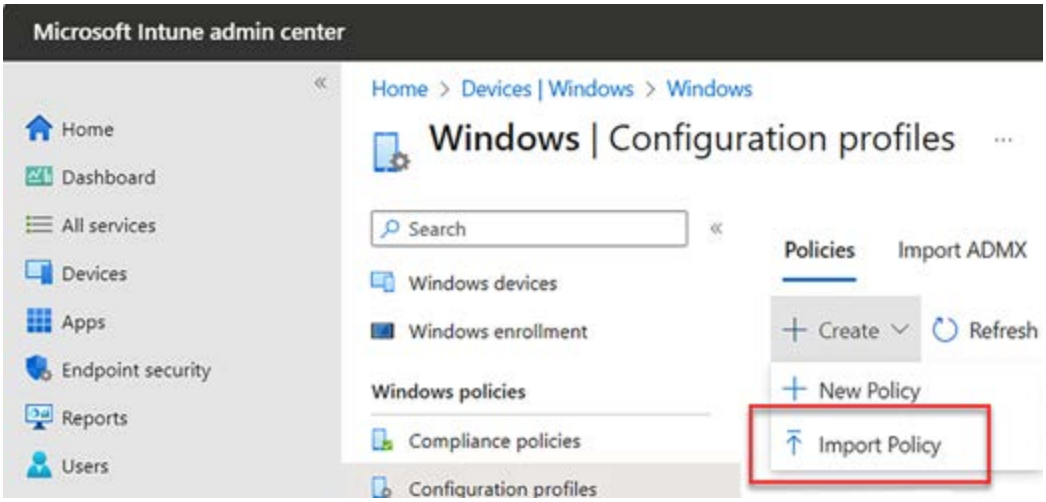


Figure 10.29: Settings catalog Import Policy

Then, you drag and drop your previous exported JSON policy files and enter a new name for the policy.

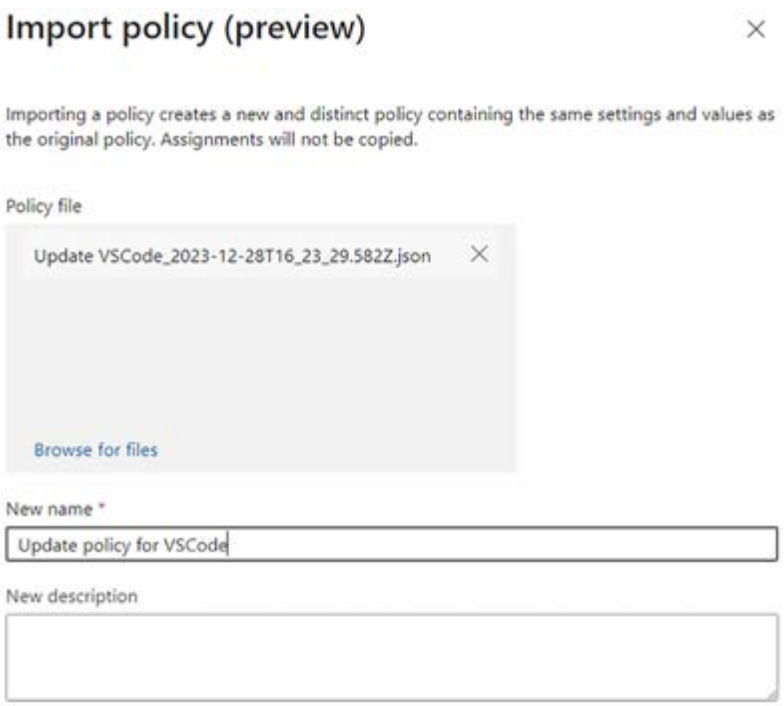


Figure 10.30: Import policy

This concludes this section on the settings catalog. In the next section, we will cover how to import ADMX into Microsoft Intune.

Importing ADMX

You can import custom and/or third-party ADMX and **Administrative Template Language** (**ADML**) templates into the Microsoft Intune admin center. Once imported, you can create a device configuration policy using these settings, and then assign the policy to your managed Windows devices.

A good source to get the Group Policy Administrative Templates Catalog is `https://admx.help/`.

There are also some product-specific links here:

- The ADMX templates for Firefox are available for download here: `https://github.com/mozilla/policy-templates/releases`
- Download the Chrome browser for your enterprise: `https://chromeenterprise.google/browser/download/#windows-tab`
- Zoom policy templates: `https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065466#h_4028bb63-77cc-4eec-ad1e-6311ec3f1b59`

Limitations:

- 20 ADMX files is the maximum number that can be uploaded to Intune. Each file must be 1 MB or smaller.
- For each ADMX file, only one ADML file can be uploaded.
- Each ADMX file supports one language.

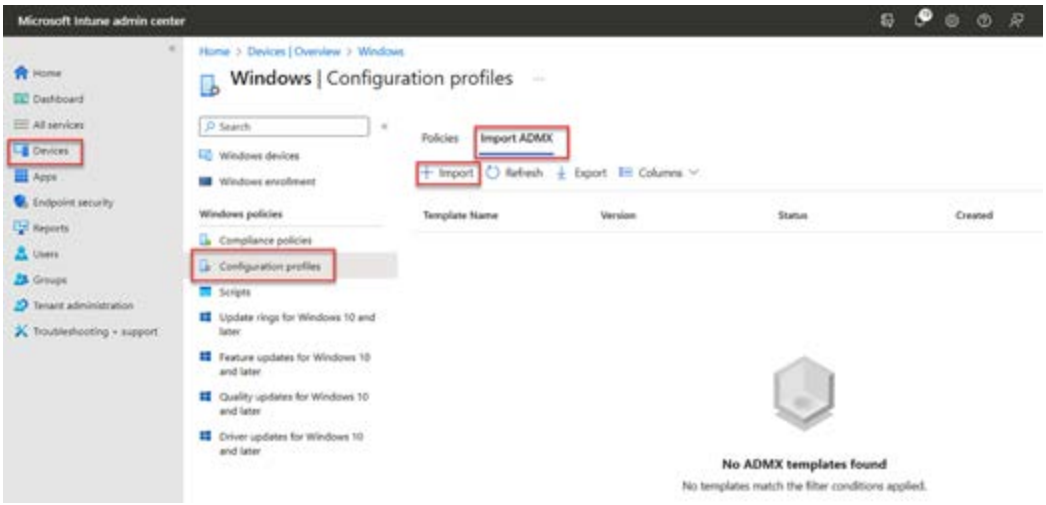


Figure 10.31: Import AMDX

Then you need to upload the ADMX files that you have previously downloaded and extracted to your local hard drive.

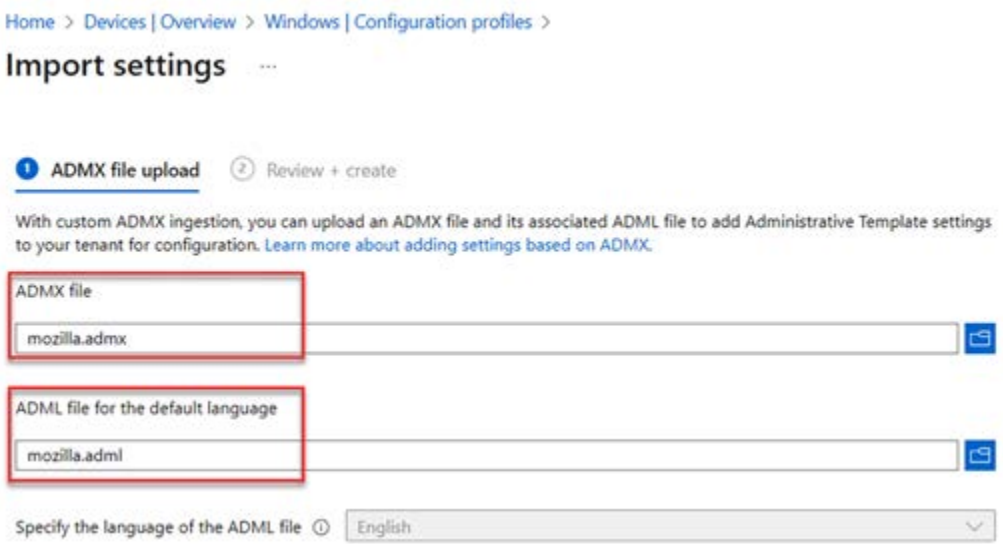


Figure 10.32: ADMX file upload

Then you have your list of ADMX files in Intune:

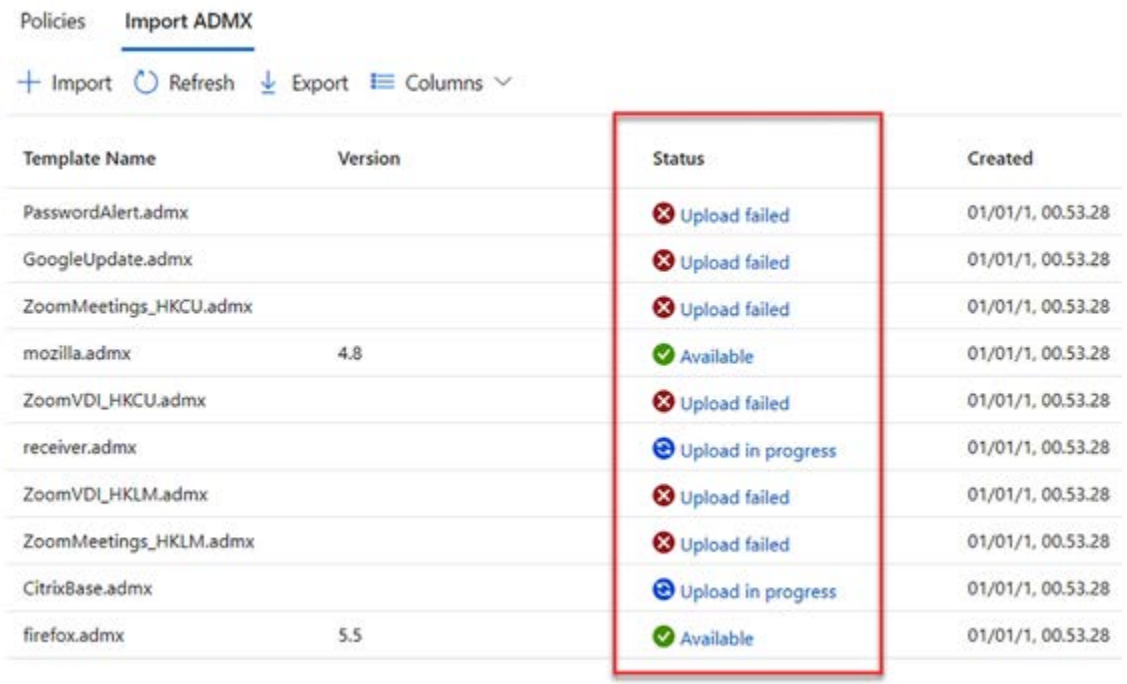


Figure 10.33: Import ADMX list

If the upload fails, you need to look at the error details and fix the error. By clicking on the **Upload failed** error, you will get the error details as you see below.

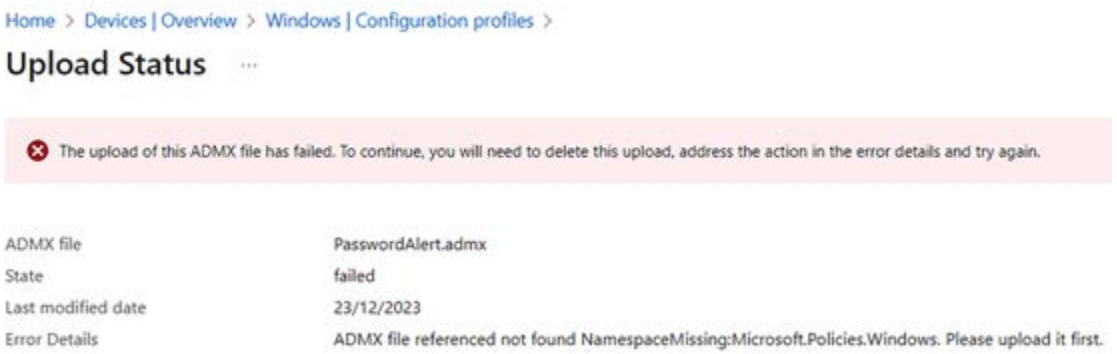


Figure 10.34: Import error

To see if your ADMX has a dependency, open the ADMX file in a text editor and look for `using prefix` in the `policyNamespaces` node. Any dependencies will be listed.

In the following example, the `PasswordAlert.admx` file requires the `Windows.admx` file:

```
<policyNamespaces>
  <target prefix="Password Alert" namespace="V1.34" />
  <using prefix="windows" namespace="Microsoft.Policies.Windows" />
</policyNamespaces>
```

You need to remove the following:

```
<using prefix="windows" namespace="Microsoft.Policies.Windows" />
```

Then you can re-upload it and it will work.

When you have fixed the issues in the ADMX files, you will have them all uploaded without errors.

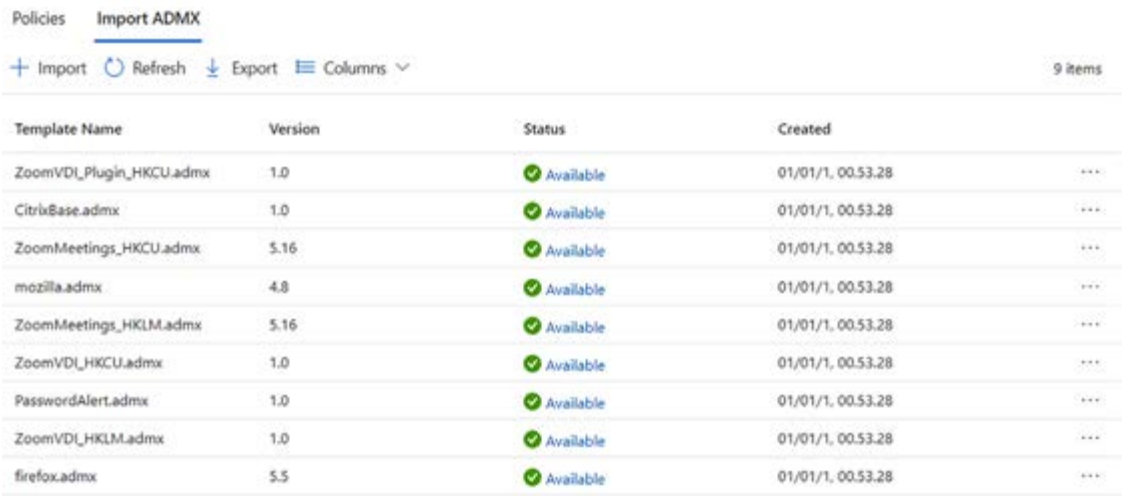


Figure 10.35: ADMX list available

Create a new Windows policy with the profile type **Templates** and the template name **Imported Administrative Templates**.

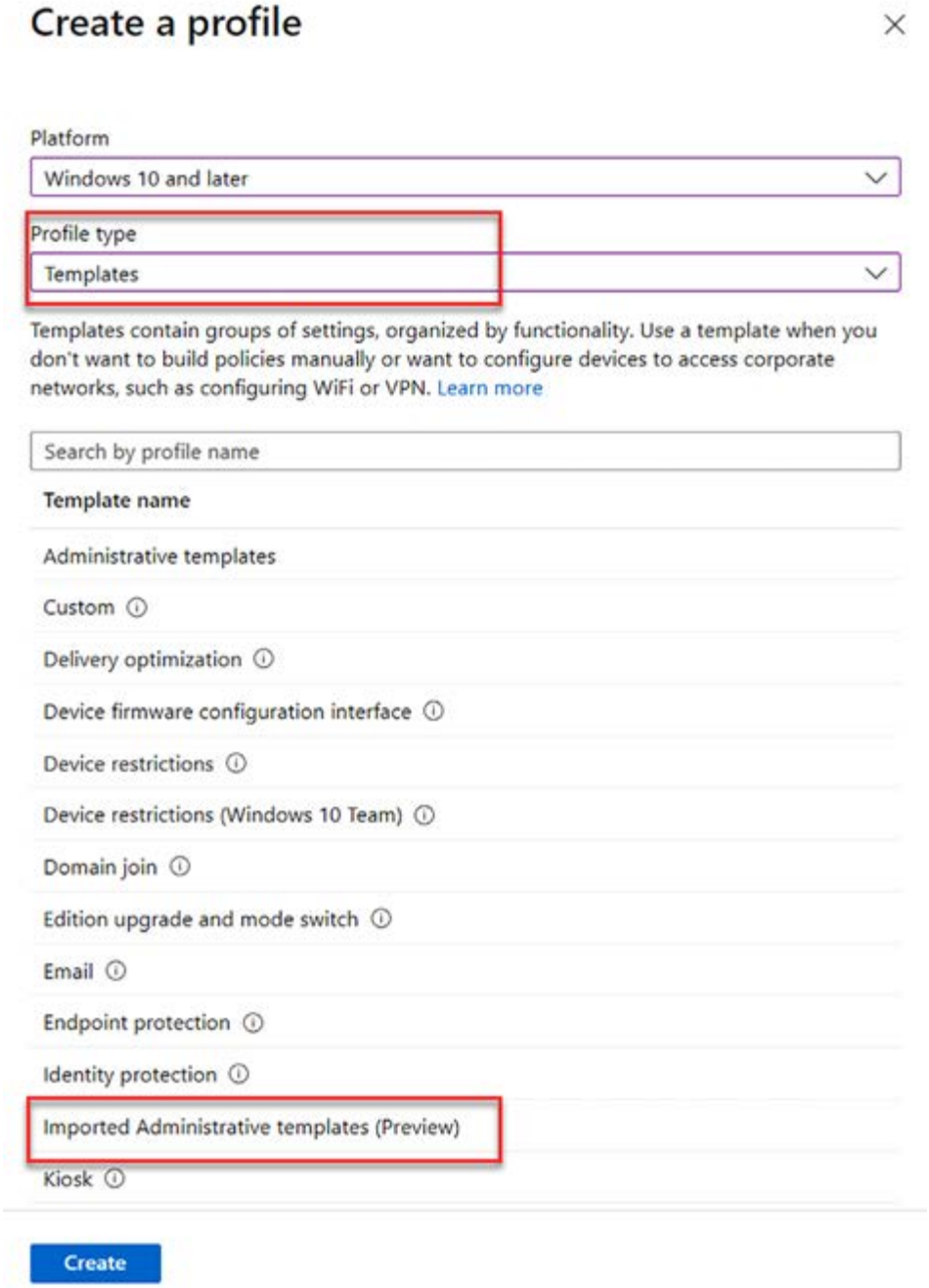


Figure 10.36: Imported Administrative templates

Then you can browse and configure **Computer Configuration** for all the imported ADMX.

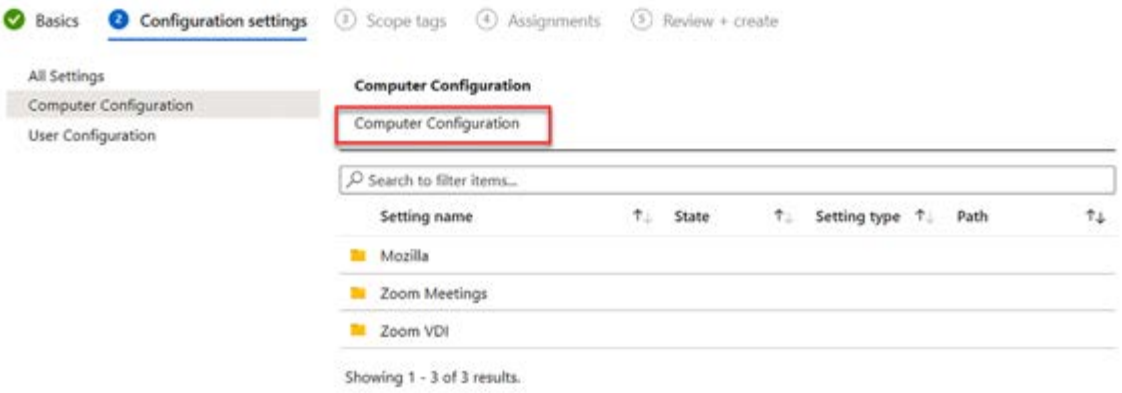


Figure 10.37: ADMX Computer Configuration

And you can browse and configure **User Configuration** for all the imported ADMX.

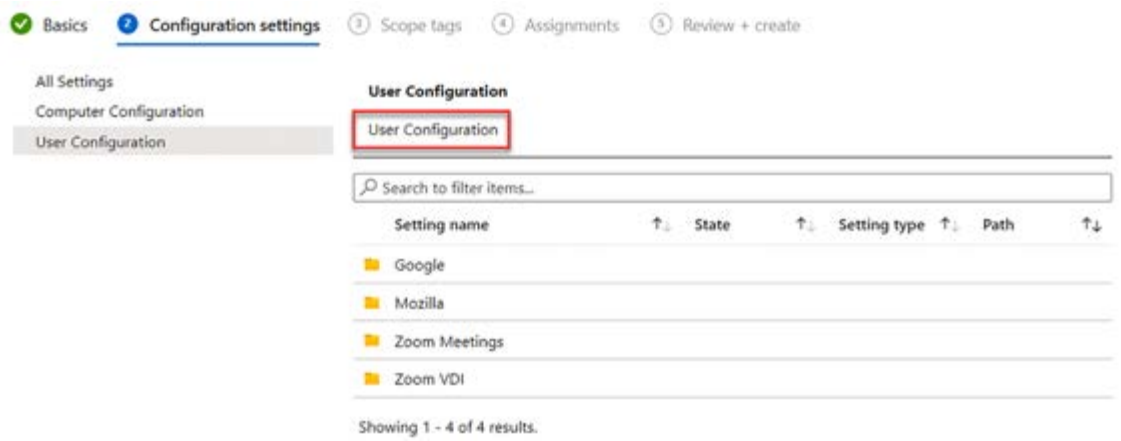


Figure 10.38: ADMX User Configuration

You can browse and configure the specific policy setting that you need inside the ADMX-based policy.

In this example, import the **Enterprise Roots** certificate from the Windows certificate store into Firefox.

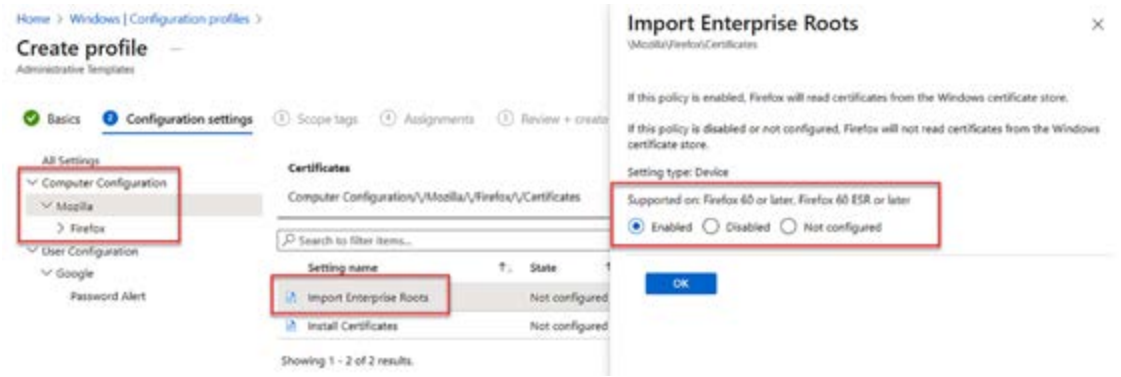


Figure 10.39 – ADMX Import Enterprise Roots

This concludes this section on importing ADMX. In the next section, we will cover how to configure administrative templates from within Microsoft Intune.

Configuring administrative templates

Administrative templates include thousands of settings that control features in Microsoft Edge version 77 and later, Internet Explorer, Microsoft Office, Remote Desktop, OneDrive, passwords, PINs, and more. These settings allow IT pro administrators to manage group policies using Microsoft Intune in the cloud.

The Windows settings are GPO settings that you already know about from **Active Directory** (**AD**). These settings, which are built into Windows, are ADMX-backed settings that use XML. The Office and Microsoft Edge settings are ADMX-ingested and use the ADMX settings in Office administrative template files and Microsoft Edge administrative template files.

Not all ADMX policies are whitelisted in all Windows versions, so it is a good idea to keep your version of Windows as current as possible in your organization. To verify what ADMX policies are supported on the Windows build you are running, check the Windows policy CSP documentation: `https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider#policies-supported-by-group-policy-and-admx-backed-policies`.

To configure the template, follow these steps:

1. In the Microsoft Intune admin center, go to **Home | Devices | Windows | Configuration profiles** and apply the following:
    - **Platform:** Select **Windows 10 and later**
    - **Profile type:** Select **Templates**
    - **Template name:** Select **Administrative templates:**

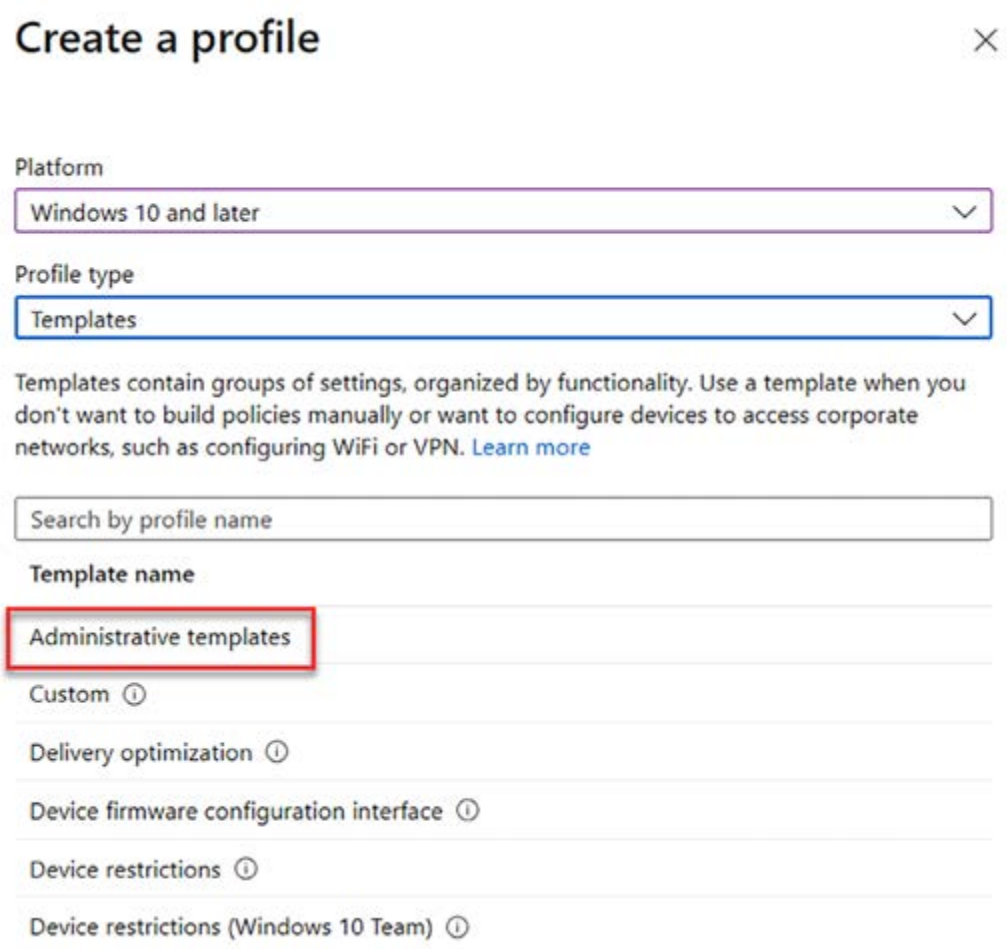


Figure 10.40: Creating Administrative templates

2. When creating a profile in Microsoft Intune, the name is a mandatory field. You should enter a name that indicates what the policy does. Now you can select **All Settings**, **Computer Configuration**, or **User Configuration**, depending on what you want to configure. In this case, we will configure the Microsoft Edge browser.

3. Under **Computer Configuration**, you can find all the top-level categories, such as **FSLogix:**

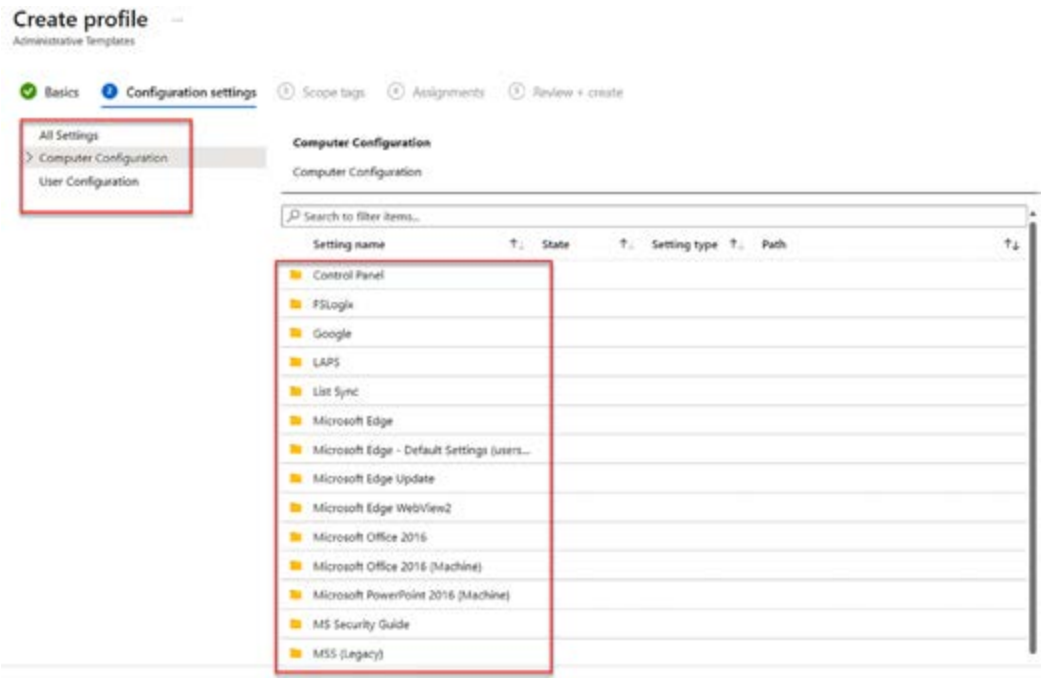


Figure 10.41: Computer Configuration

We will not give you any policy examples for administrative templates as the settings catalog is the best option for policy creation, including ADMX-based ones.

This concludes the section on administrative templates. Next, we will cover how to leverage administrative templates in Microsoft Intune to configure OneDrive Known Folder Move.

OneDrive Known Folder Move configuration

The Settings Catalog also includes Administrative templates that could be used to configure Microsoft OneDrive **Known Folder Move** (**KFM**).

Here are the two primary advantages of leveraging Windows known folders (**Desktop**, **Documents**, **Pictures**, **Screenshots**, and **Camera Roll**) in Microsoft OneDrive for the users in your Microsoft 365 environment:

- Your end users can continue using the folders they are familiar with. They do not have to change the way they do their daily work to save files to OneDrive.

- Saving files to OneDrive backs up your users' data in the Microsoft 365 backend in OneDrive, and the end user can access their data from anywhere on any device:



Figure 10.42 – Manage protection of important folders

To configure OneDrive KFM, you can create an administrative template profile in Microsoft Intune. Start by giving the profile a name:

- **Name:** Enter `OneDrive Know Folder Move`

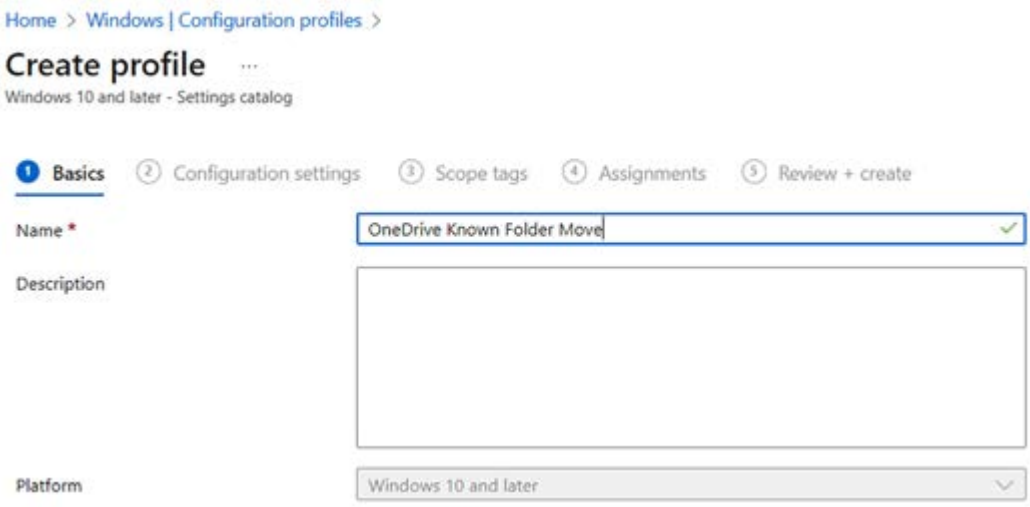


Figure 10.43 – Settings catalog – OneDrive KFM

Search for **OneDrive | Settings picker** and add all settings by clicking on **Select all these settings.**

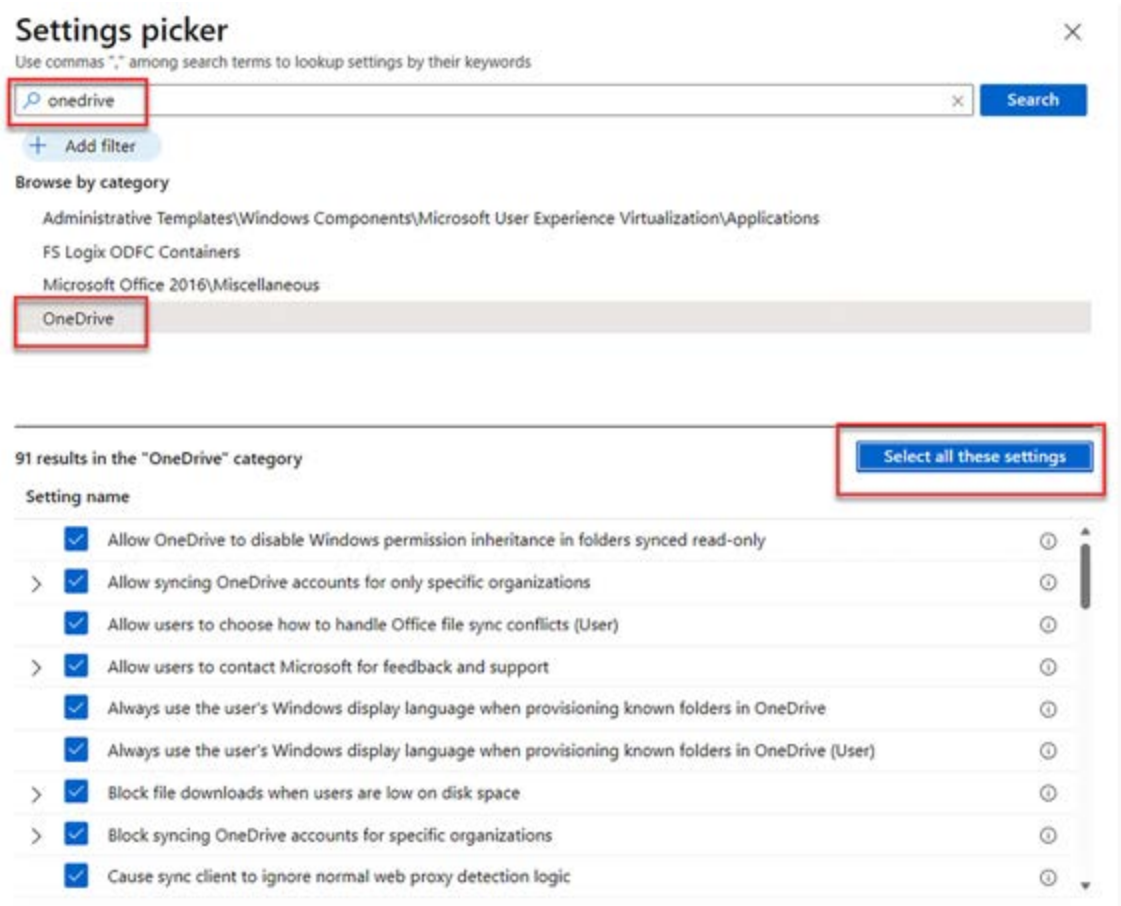


Figure 10.44: Settings catalog – Add OneDrive

There are a few settings that you need to configure to silently configure OneDrive KFM for the end user:

- For **Silently sign in users to the OneDrive sync app with their Windows credentials**, select **Enabled:**



Figure 10.45 – Silently sign users in to OneDrive

This setting lets you silently sign in users to the OneDrive sync app (`OneDrive.exe`) with their Windows credentials. If you enable this setting, users who are signed in on the PC with the Entra ID account can set up the sync app without entering the credentials for the account. Users will still be shown **OneDrive Setup** so they can select folders to sync and change the location of their OneDrive folder. This setting is frequently used together with **Set the maximum size of a user's OneDrive that can download automatically** on PCs that don't have **Files On-Demand**, and **Set the default location for the OneDrive folder**. If you disable or do not configure this setting, users will need to sign in with their work or school account to set up sync.

To configure Windows known folders to automatically be moved to OneDrive for Business, you need to configure the following settings:

- **Silently move Windows known folders to OneDrive:** Select **Enabled.**
- **Tenant ID:** Use the tenant ID from your Microsoft 365 tenant.
- **Show notification to users after folders have been redirected: No**
- You can also configure the folders that you want to sync: In this case, **Desktop**, **Documents**, and **Pictures.**

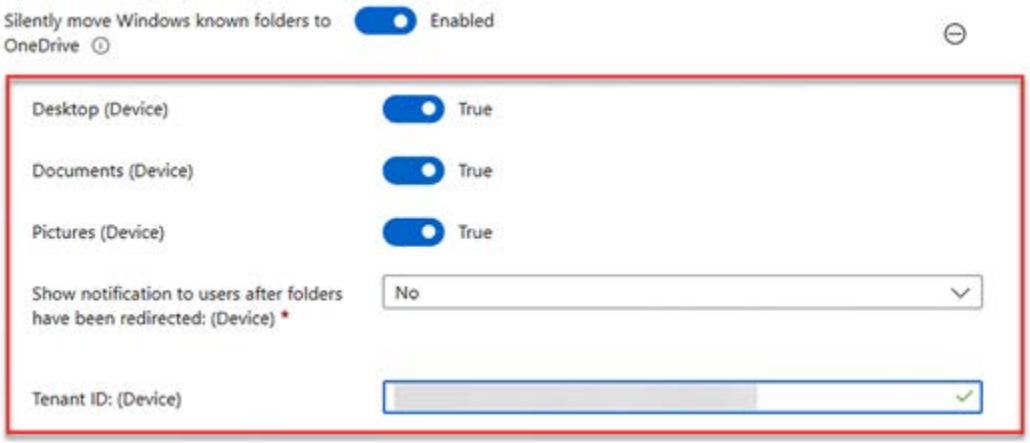


Figure 10.46: Silently move Windows known folders to OneDrive

To find your Tenant ID, you can go to the Entra ID admin center (`https://entra.microsoft.com`). You can find it under **Overview** | **Basic information** | **Tenant ID.**

You can also find your Tenant ID, which is unique for your organization:

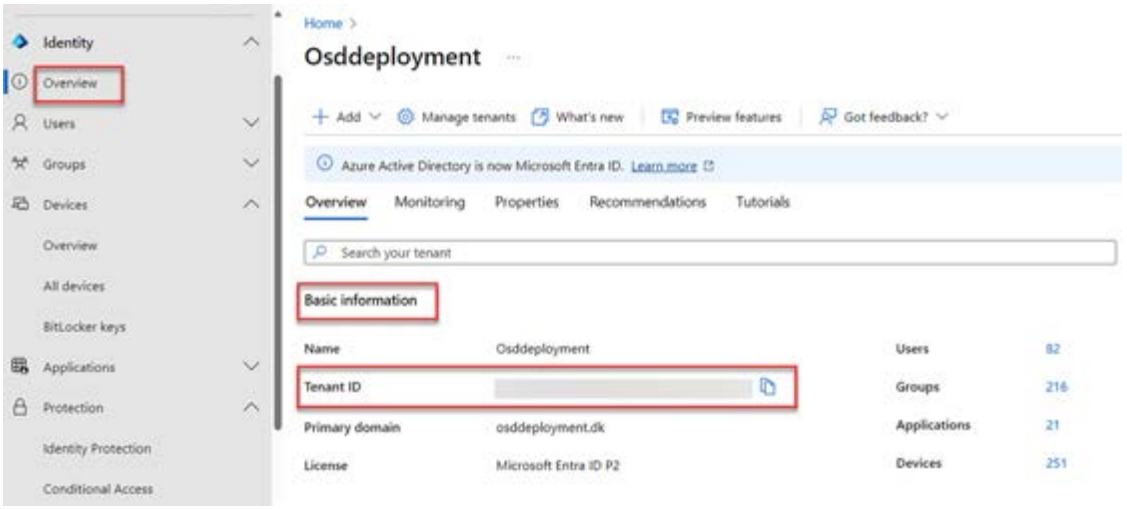


Figure 10.47: Tenant ID in the Entra ID admin center

OneDrive – block syncing specific file extensions

One of the main key releases customers have been waiting for has been the ability to exclude files, folders, and extensions from syncing. This is something I will explain in more depth in this section, plus some more tips and tricks for the use of OneDrive.

This setting lets you enter keywords to prevent uploading certain files to OneDrive. You can enter complete names, such as `setup.exe`, or use the asterisk (*) as a wildcard character to represent a series of characters.

In this example, it is `.lnk` files that will be excluded from syncing to OneDrive for Business.

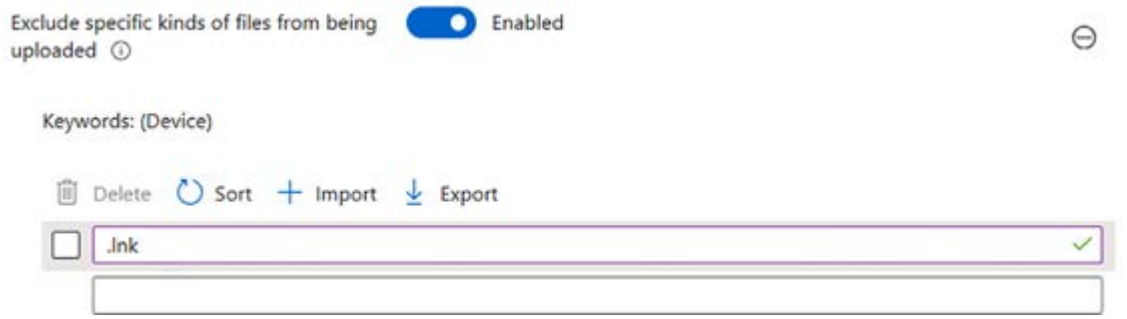


Figure 10.48: Exclude specific kinds of files from being uploaded

If you enable this setting, the sync app doesn't upload new files that match the keywords you specified. No errors appear for the skipped files, and the files remain in the local OneDrive folder. The OneDrive sync app must be restarted after this setting is enabled for the setting to take effect. If you disable or do not configure this setting, the sync app uploads all supported files in all synced folders.

You can assign your OneDrive KFM policy to a device group.

This concludes this section on administrative templates. Next, we will walk through some of the many different options for device configuration with templates in Microsoft Intune.

Configure device configuration (template)

Templates contain groups of settings, organized by functionality. You should use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring Wi-Fi or VPN.

We will show some examples, along with use cases, in this section.

The first example is **Device Firmware Configuration Interface**. Here, it is recommended that if you have devices that support **Device Firmware Configuration Interface** (**DFCI**), bear in mind that it requires that the device is registered through the Autopilot service from the CSP or OEM process. Read more about that in *Chapter 7*. DFCI enables Windows to pass management commands from Intune to **Unified Extensible Firmware Interface** (**UEFI**). In Intune, use this feature to control BIOS settings. Typically, firmware is more resilient to malicious attacks. It limits end users' control over the BIOS, which is good in a compromised situation. For example, you use devices running Windows 10 or later in a secure environment and want to disable the camera. You can disable the camera at the firmware layer, so it doesn't matter what the end user does. Reinstalling the OS or wiping the computer won't turn the camera back on. In another example, lock down the boot options to prevent users from booting up another OS, or an older version of Windows that doesn't have the same security features:

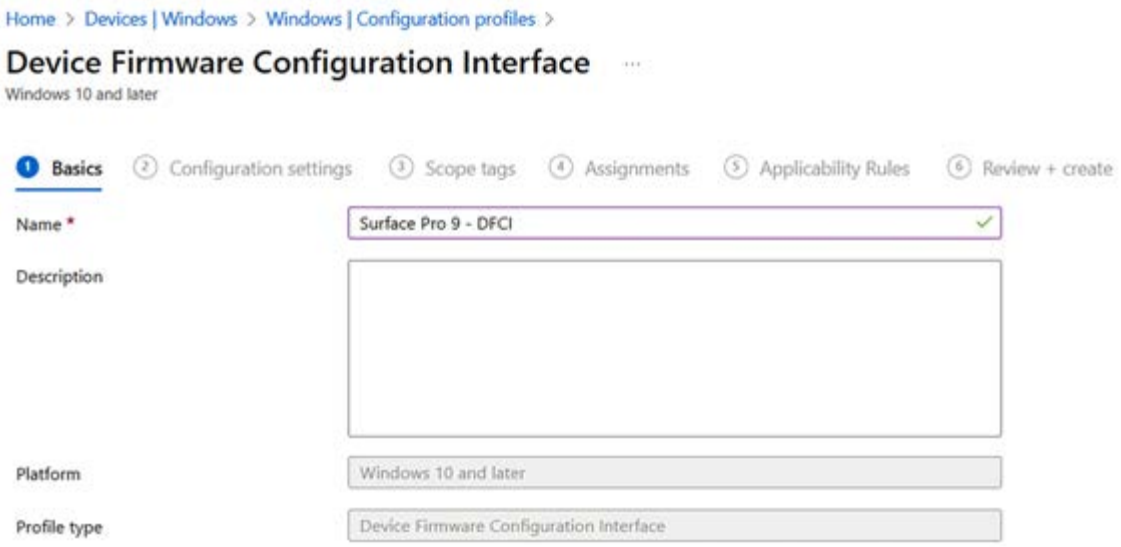


Figure 10.49 – Templates – DFCI

You can start by configuring **Allow local user to alter UEFI settings**, where you can set it to **None** and all settings are managed by Microsoft Intune, or **Only not configured settings**, which means that the end user can change all settings in the UEFI that are not configured by Microsoft Intune:

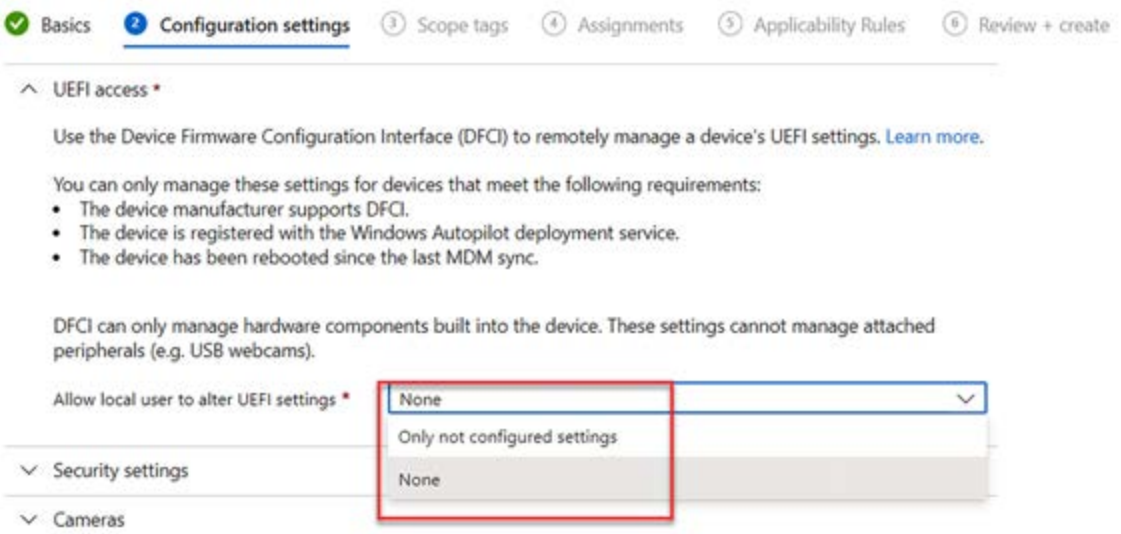


Figure 10.50: DFCI – Allow local user

This disables all internal cameras on the device but leaves the Windows Hello for Business camera enabled. There are customers where this is important if the devices are not allowed to take pictures in a restricted area.

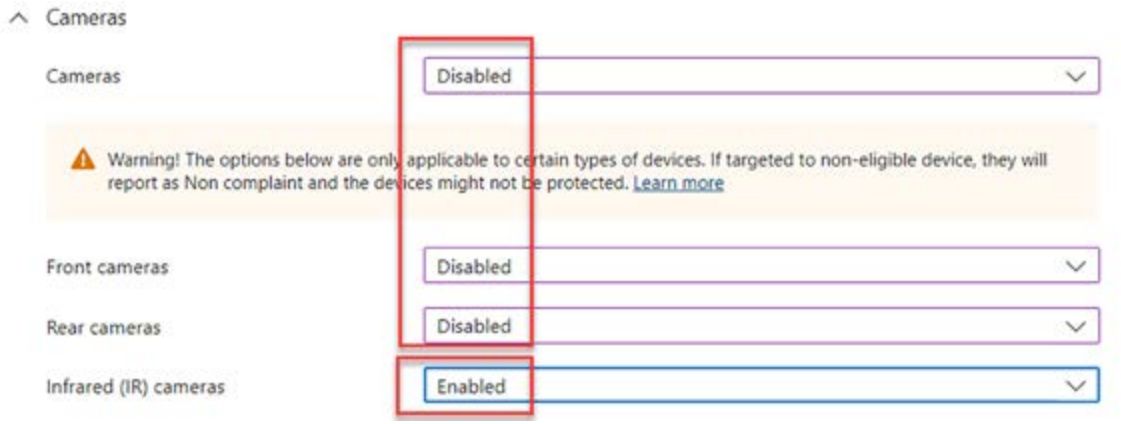


Figure 10.51: DFCI – Disable camera

You can also block external media and network adapters from booting on the device if that is your requirement.



NOTE

Disabling all external boot options or all external ports significantly complicates OS recovery. To recover a device that can no longer boot Windows, you may have to physically open the device and replace the hardware storage.

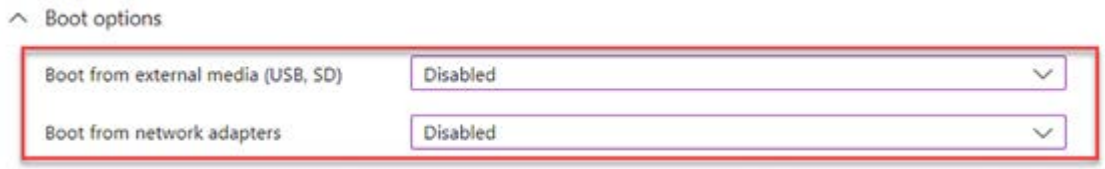


Figure 10. 52: DFCI – Disable Boot options

When the end user goes into the UEFI, they will see **Some settings are managed by your organization** and will not be able to change them – here is an example from a Surface device:

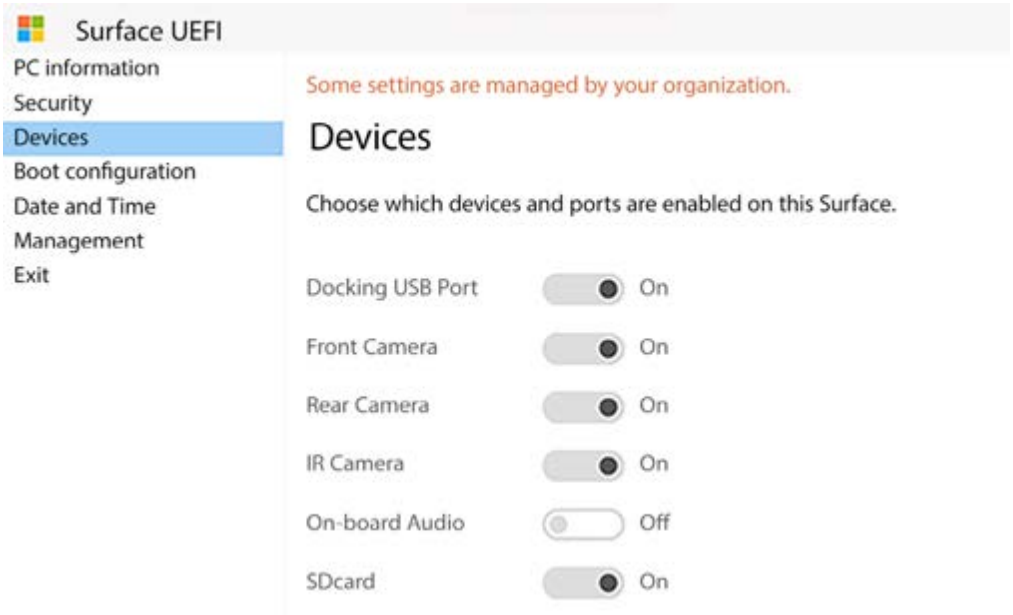


Figure 10.53: Surface – DFCI settings

Then, configure all the settings, test them, and evaluate whether the configuration meets all the requirements in your organization.

Leveraging a custom policy as a last resort

Only use a custom policy as a last resort. It is not always easy to create a custom policy. You need to know where, how, and why the CSP is working. Support for custom policies is also a way to provide 0-day support for new policies in new OSs or Windows insider builds.

In this scenario, we will create a custom OMA-URI policy that configures **Config Lock**.

Secured-core **Configuration Lock** (**Config Lock**) is a new feature of secured-core PCs that prevents configuration drift from secured-core PC features caused by unintentional misconfiguration. In other words, it ensures that a device intended to be a secured-core PC remains a secured-core PC. **Config Lock** enables IT administrators to prevent configuration drift and keep the OS configuration in the desired state. With Config Lock, the OS monitors the registry keys that configure each feature and when it detects a drift, reverts to the IT-desired state in seconds.

Follow these steps to create a custom profile with a template in Microsoft Intune:

1. For **Profile type**, select **Templates**. For **Template name**, select **Custom**. Then, click **Add**:

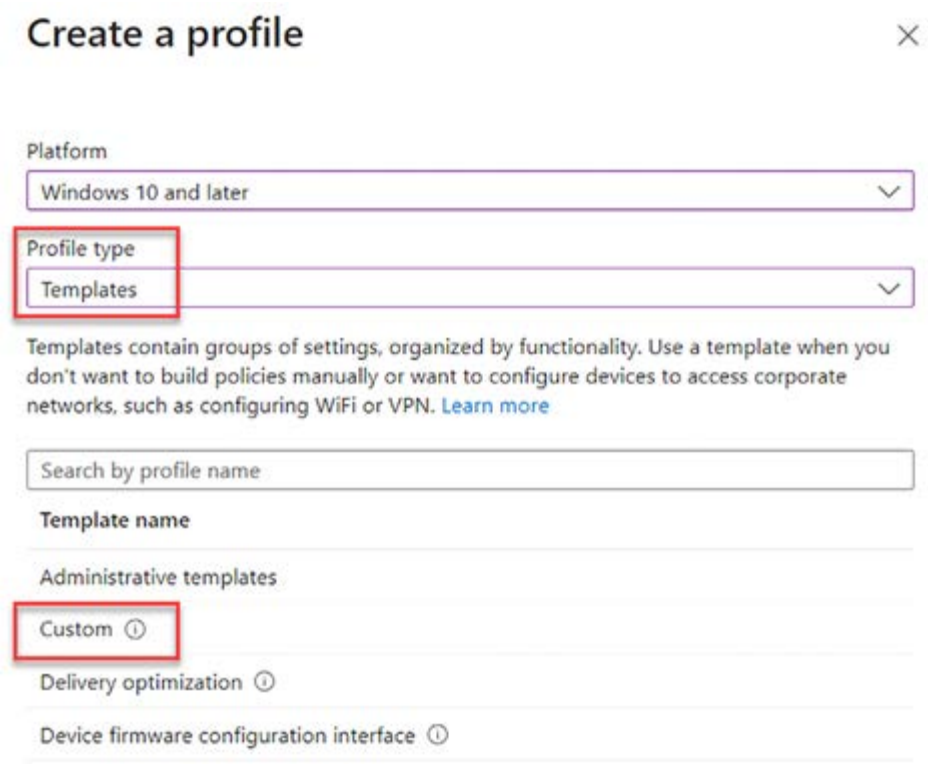


Figure 10.54: Templates – Custom

2. By clicking **Add**, you can fill out all the required values in the **Add row** blade. You can add as many rows as you need to the policy you are creating:

    - **Name: Enable Config Lock**
    - **Description: Enables IT to "lock" secured-core PC features when managed through MDM**
    - **OMA-URI:** Enter the following path, which is case-sensitive, and avoid trailing spaces: `./Vendor/MSFT/DMClient/Provider/MS%20DM%20Server/ConfigLock/Lock`

- **Data type:** Select **Integer**
  - Data types can be:
    - `Base64 (file) Boolean`
    - `String (XML file)`
    - `Date and time`
    - `String`
    - `Floating point`
    - `Integer`
- **Value: 1**

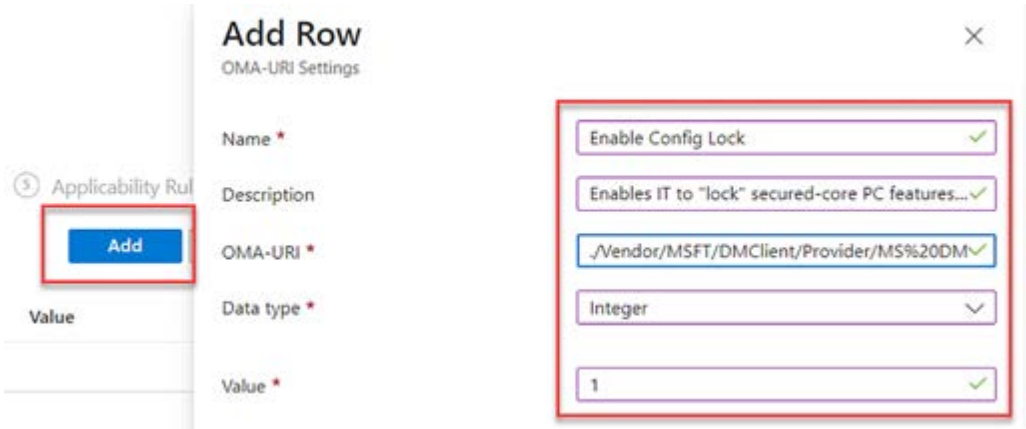


Figure 10.55: OMA-URI settings

This concludes this section on custom policies. The need for custom policies will reduce as the capacity of the settings catalog is expanding all the time.

Config Refresh

Config Refresh is a feature that allows you to set a cadence for Windows devices to reapply previously received policy settings. This ensures that your settings are retained the way you configured them. The feature can be used to configure a refresh cadence in which the already received configuration policies will be refreshed, no matter whether the device is online or offline. The default Config Refresh cadence is every 90 minutes if the policy is configured and deployed to devices, but it can be set to every 30 minutes if desired.

The normal policy refresh cycle is 8 hours as that is the MDM sync interval.

To create a profile that enables Config Refresh, open the Microsoft Intune admin center:

Go to **Home** | **Devices** | **Windows** | **Configuration profiles** | **Create New policy** and apply the following:

- **Platform:** Select **Windows 10 and later**
- **Profile type:** Select **Settings catalog**

- Search for **Config Refresh** in the settings picker:

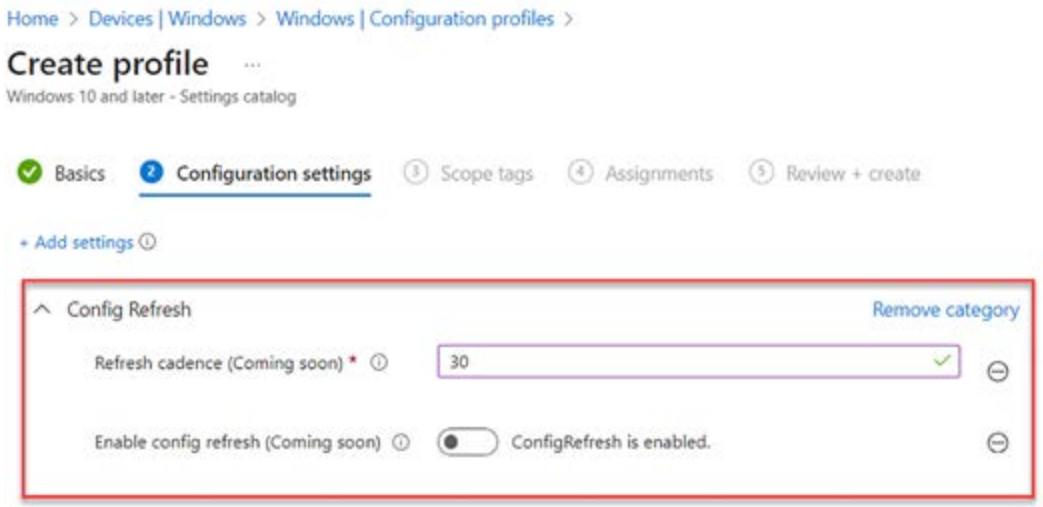


Figure 10.56: Config Refresh

Configure the refresh cadence from 30 to 1,440 minutes – we have chosen 30 minutes in this case. Then enable Config Refresh (the policy setting is disabled by default).

In the next section, we will cover the option of running PowerShell scripts from Microsoft Intune to set device configurations.

Pushing PowerShell scripts – scripted actions to endpoints

If there is no policy for the configuration change that you need to make on your corporate devices, you can leverage PowerShell scripts in Microsoft Intune. This is also a good way of publishing one-time installations or custom-scripted actions to both your physical and cloud endpoints. In this scenario, we will configure **Set time zone automatically** to **On**. It also requires location services to be turned on. Take a look at *Chapter 16* to see how to enable location services on your devices.

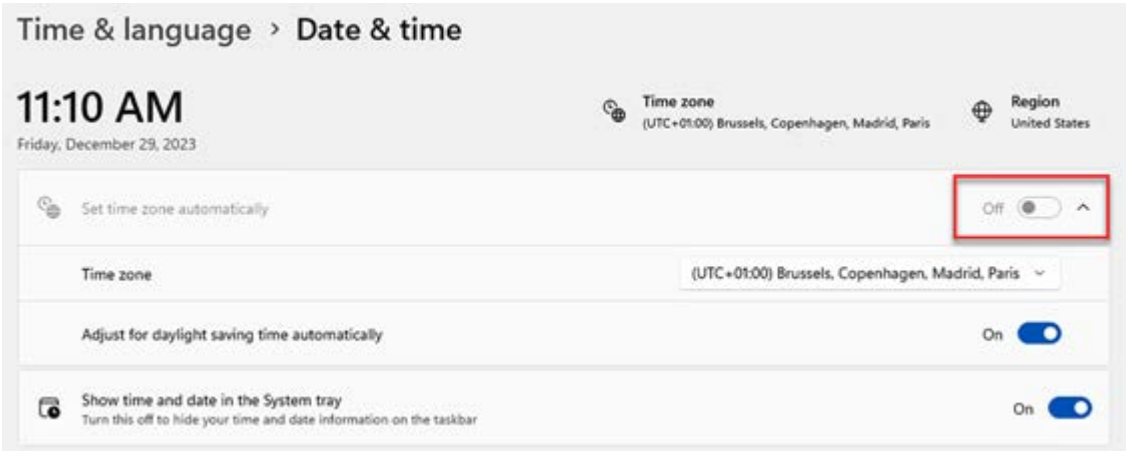


Figure 10.57: Set time zone automatically is set to Off

We can leverage a PowerShell script option to configure the registry value that changes it to **On** as there is currently no Windows policy to configure it:

1. In the Microsoft Intune admin center, browse to **Home | Devices | Windows | Scripts | Platform scripts** and click **Add:**

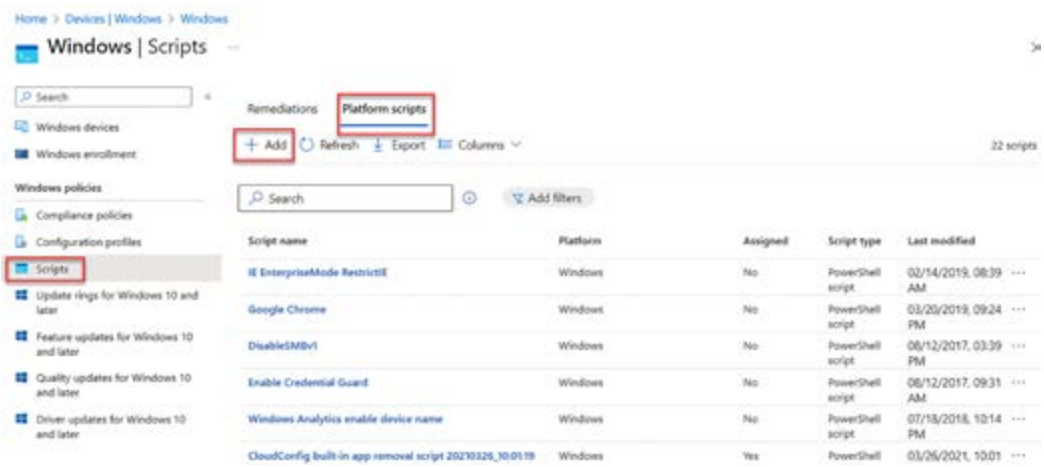


Figure 10.58: PowerShell scripts

2. Click **Select a file** to upload your PowerShell script to Microsoft Intune:



NOTE

Make sure to select **Run script in 64 bit PowerShell Host** for the right registry location.

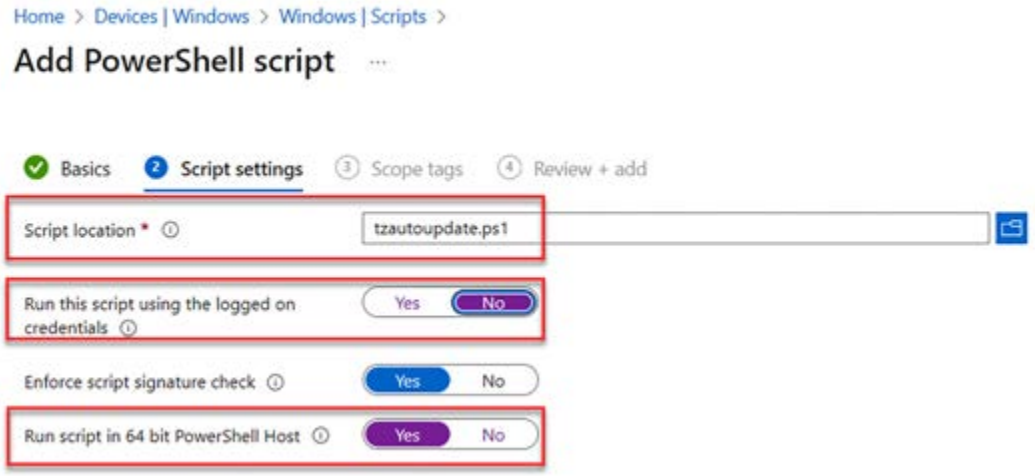


Figure 10.59: Uploading a PowerShell script

Assign the script to the user or device groups. The script will then run once on each assigned device. Here are some script examples:

- **Set time zone automatically:**

```
# Set variables to indicate value and key to set
$RegistryPath = 'HKLM:\SYSTEM\CurrentControlSet\Services\tzautoupdate'
$Name         = 'Start'
$Value        = '3'
# Create the key if it does not exist
If (-NOT (Test-Path $RegistryPath)) {
  New-Item -Path $RegistryPath -Force | Out-Null
}
# Now set the value
New-ItemProperty -Path $RegistryPath -Name $Name -Value $Value -PropertyType
DWORD -Force
```

After the PowerShell scripts have run on the device, **Set time zone automatically** is set to **On:**



Figure 10.60: Set to On

Multi admin approval

For PowerShell scripts, you can also leverage a multi admin approval workflow in Microsoft Intune so that an IT admin cannot deploy PowerShell scripts to devices without another IT admin having approved it:

1. In the Microsoft Intune admin center, browse to **Home** | **Tenant administration** | **Multi Admin Approval** | **Access policies** and click **Create:**

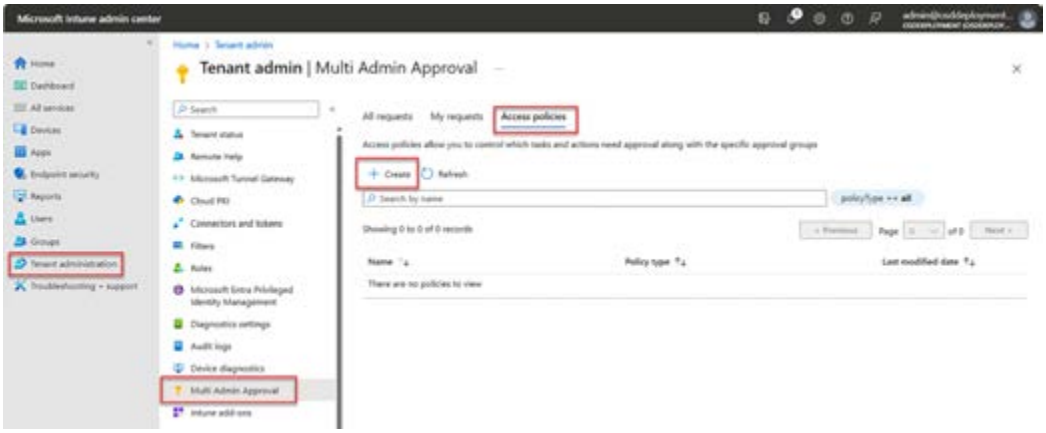


Figure 10.61: Multi Admin Approval

2. Then you need to give the access policy a name and keep the default profile type as **Script**.
3. A script policy will limit actions on a script, such as PowerShell scripts or remediation scripts. These could include create, edit, assign, and delete.
4. You need to select a group of approvers:

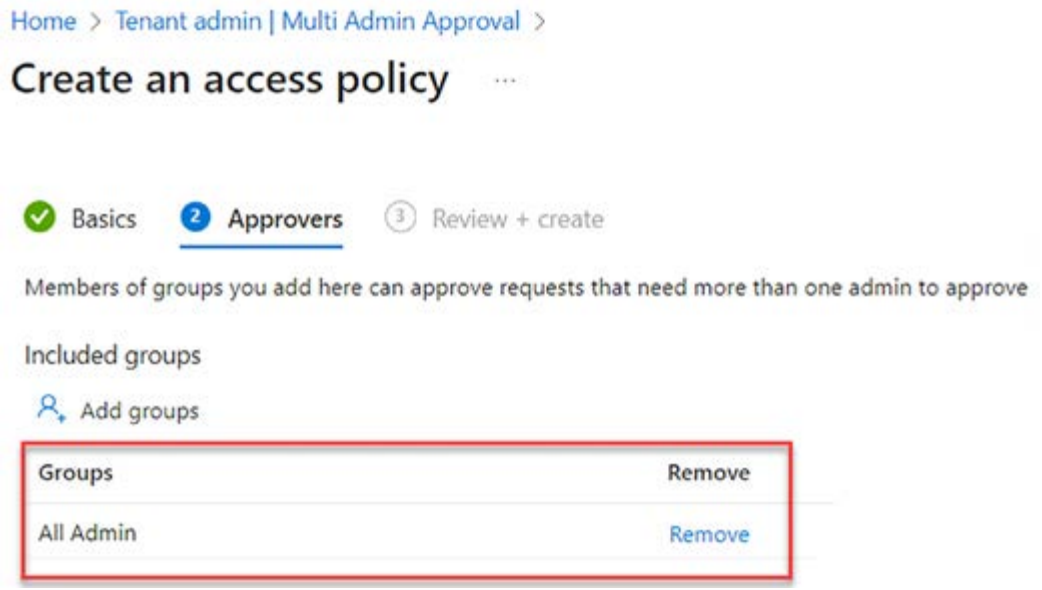


Figure 10.62: Multi Admin Approval Approvers

When you create a new PowerShell script, you do not have the **Assign** step in the workflow but you will need to add a business justification:

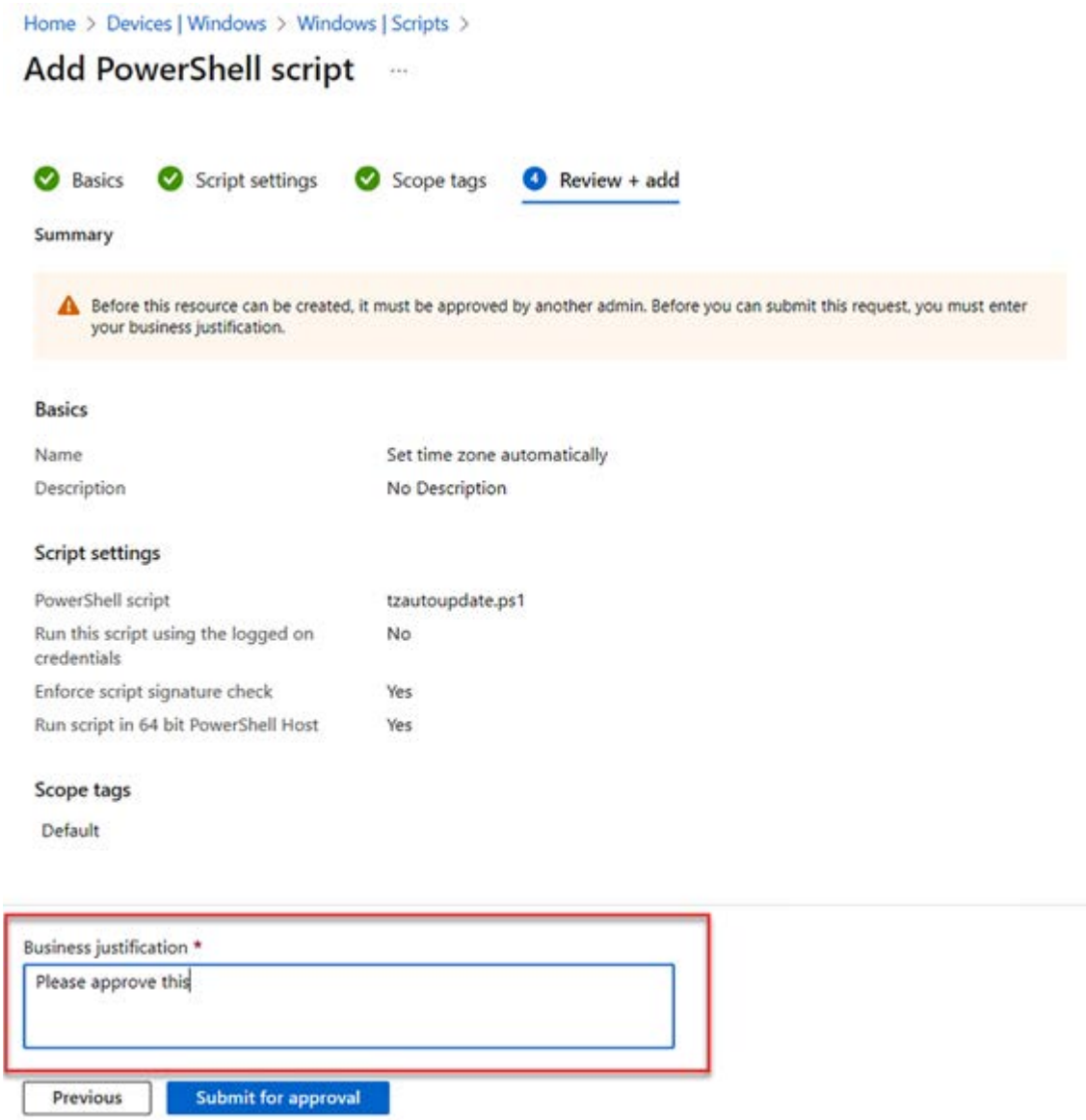


Figure 10.63: Business justification

In the **Multi Admin Approval** blade, you will see **All requests** and **My requests**

My requests is where you can see the status of your own requests. **All requests** is where you will see your own requests and the requests of other IT admins that have created a script that needs to be approved.

You need to click on the business justification to approve it.

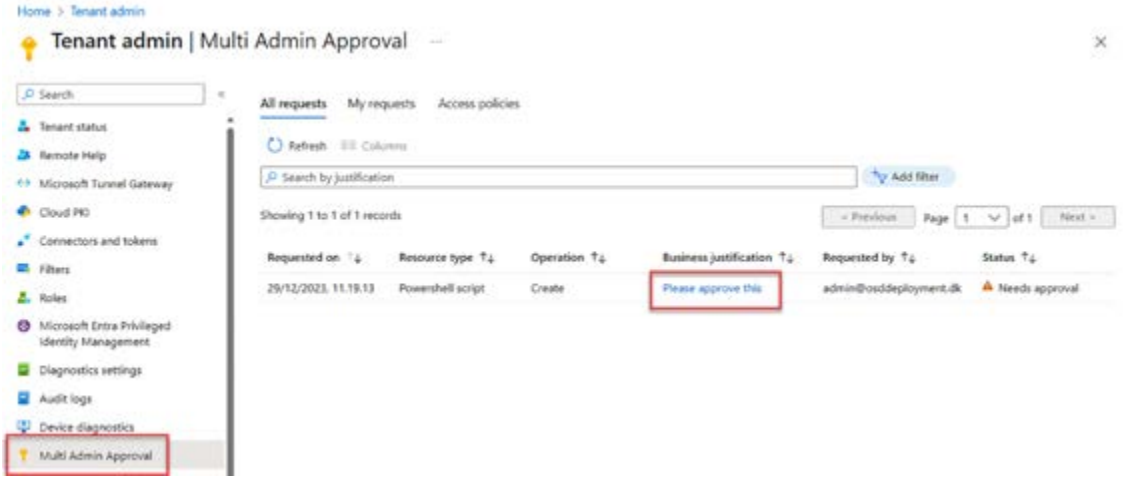


Figure 10.64: Request list

Then the IT admin can either complete the request or cancel the request.

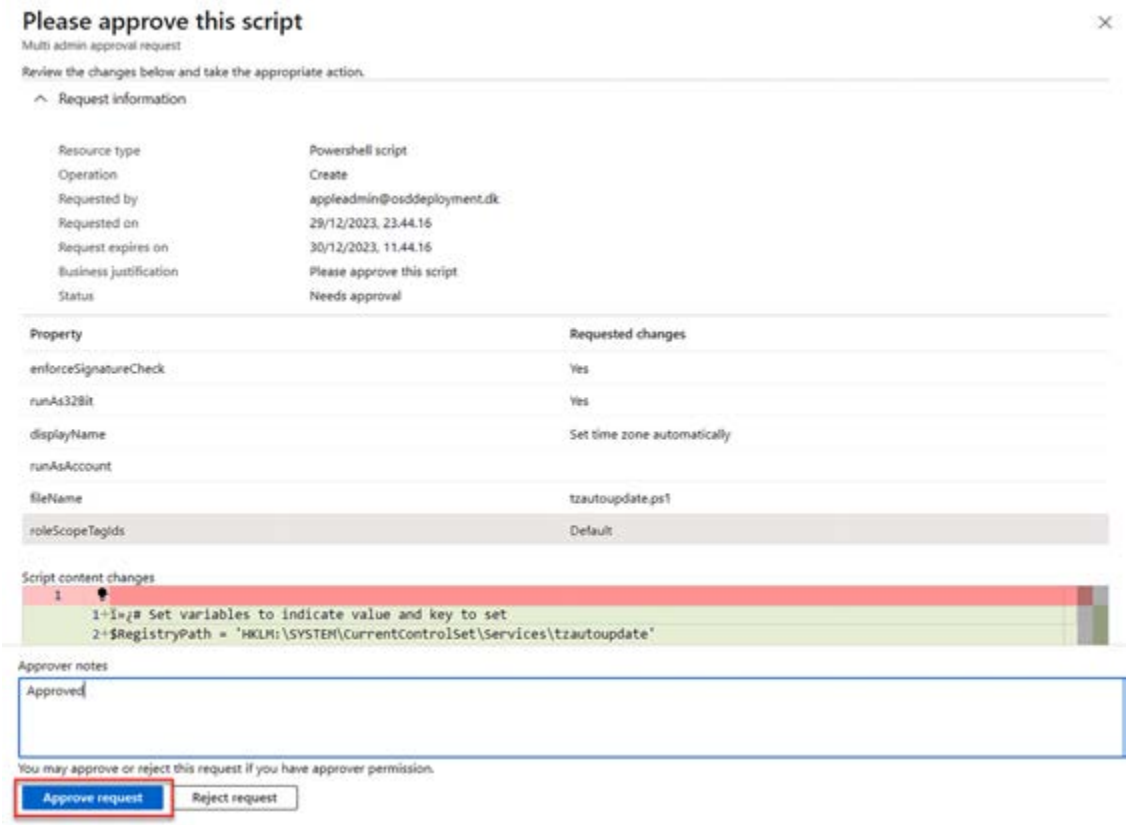


Figure 10.65: Approve request

You cannot approve your own request. In this case, if another IT admin signs in, then the request can be approved by them. These are just examples of leveraging PowerShell scripts to configure an Intune-managed Windows device. Next, we will cover compliance policies.

Compliance policies

Microsoft Intune can set a compliance state on a device. There are two possible outcomes for a device: compliant or noncompliant.

In Microsoft Intune, you can define the rules and settings that users and devices must meet to be compliant. If Conditional Access has been configured, then users and devices that are noncompliant can be blocked from accessing resources that contain corporate data.

If you are using Conditional Access to block noncompliant devices that are not Intune-managed, it also requires an Entra ID Premium license.

There are two types of compliance policies in Microsoft Intune:

- **Compliance policy settings**: Tenant-wide settings that act like a built-in compliance policy that every device receives. The compliance policy settings set a baseline for how the compliance policy will work in your Microsoft Intune environment.

  These settings configure the way the compliance service treats devices. Each device evaluates these as a **Built-in Device Compliance Policy**, which is reflected in device monitoring.

  The following are the options you can configure in the built-in policy:

  - Mark devices with no compliance policy assigned as **Default value is Compliant**. This means that this security feature is disabled by default. It is recommended that you change this setting to **Not Compliant** so that all devices without a compliance policy will automatically be marked as noncompliant.
  - **Enhanced jailbreak detection**: **Default value Disabled** (applies only to iOS/iPadOS).
  - **Compliance status validity period** (**days**): The default value is 30 days.

  Specify a period in which devices must successfully report on all their received compliance policies. If a device fails to report its compliance status for a policy before the validity period expires, the device is treated as noncompliant. You can configure a period so that it ranges from 1 to 120 days.

  To manage the compliance policy settings, sign in to the Microsoft Intune admin center and go to **Endpoint security** | **Device compliance** | **Compliance policy settings**.

- **Device compliance policy**: Platform-specific rules you configure and deploy to groups of users or devices. These rules define requirements for devices, such as the minimum number of operating systems or the use of disk encryption. Devices must meet these rules to be considered compliant.

Windows compliance policy

In this section, we will only cover the Windows compliance policy and no other support platforms in Microsoft Intune.

The **Device Health Attestation** (**DHA**) and **Microsoft Azure Attestation** (**MAA**) services validate the **Trusted Platform Module** (**TPM**) and **Platform Configuration Register** (**PCR**) logs for a device and then issue a DHA report. Microsoft offers the DHA cloud service, a Microsoft-managed DHA service that is free, geo-load-balanced, and optimized for access from different regions of the world.

MAA is Windows 11 only and will provide a future-proof solution that can add more checks over time than what we have with DHA today for Windows 10.

MAA/DHA enables enterprises to raise the security bar of their organization to hardware-monitored and attested security, with minimal or no impact on operation costs.

The MAA/DHA service integrates with MDM solutions and does the following:

- Combines the information received from the MAA/DHA service on the devices (through existing MDM communication channels) with the MAA/DHA report.
- Makes more secure and trusted security decisions, based on attested hardware and protected data.
- When leveraging MAA/DHA in a compliance policy to check for BitLocker encryption, Windows must be rebooted before it gets into a compliant state in Microsoft Intune.

In the **Device Health** section of the Windows compliance policy, there are three settings:



Figure 10.66 – Compliance policy – Device Health

Update these settings as follows:

- **Require BitLocker: Require** – Windows BitLocker drive encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the TPM to help protect the Windows operating system and user data. It also helps confirm that a computer isn't tampered with, even if it's left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer. This check does not check whether BitLocker is in **Suspend** mode or not. You need to leverage the option to check for encryption instead.
- **Require Secure Boot to be enabled on the device: Require** – The system is forced to boot to a factory-trusted state. The core components that are used to boot the machine must have correct cryptographic signatures that are trusted by the organization that manufactured the device. These signatures are verified by UEFI firmware before it lets the machine start. If any files are tampered with, which breaks their signature, the system doesn't boot.
- **Require code integrity**, which detects if an unsigned driver or system file is being loaded into the kernel. It also detects if a system file is changed by malicious software or run by a user account with administrator privileges.

MAA/DHA requires a reboot for the device to be compliant as the MAA/DHA certificate is hardware stored in the TPM and will only be read during boot time.

Require encryption of data storage on the device will also check for BitLocker encryption just like the MAA/DHA BitLocker encryption, but it does not require the device to reboot to be compliant. One other advantage of this setting is that it will also detect if BitLocker is suspended.



Figure 10.67: Encryption

In the **System Security** section, there is a subsection for the **Device Security** of the Windows compliance policy. Here, you can configure four settings:

- **Firewall**: Turn on the Microsoft Defender Firewall and prevent users from turning it off.
- **Trusted Platform Module (TPM): Require** – Intune checks the TPM chip version for compliance. The device is compliant if the TPM chip version is greater than 0. The device isn't compliant if there isn't a TPM version on the device.
- **Antivirus: Require** – Check compliance using antivirus solutions that are registered with Windows Security Center, such as Symantec or Microsoft Defender.

- **Antispyware: Require** – Check compliance using antispyware solutions that are registered with Windows Security Center, such as Symantec or Microsoft Defender:



Figure 10.68: Compliance policy – Device Security

In the **Defender** section of the Windows compliance policy, you can configure four settings, as shown here:

- **Microsoft Defender Antimalware: Require** – Turn on the Microsoft Defender antimalware service and prevent users from turning it off.
- **Microsoft Defender Antimalware minimum version:** Minimum version of Microsoft Defender (for example, 4.11.0.0).
- **Microsoft Defender Antimalware security intelligence up-to-date: Require** – Force the Microsoft Defender security intelligence to be up-to-date.
- **Real-time protection: Require** – Turn on real-time protection, which scans for malware, spyware, and other unwanted software:



Figure 10.69: Compliance policy – Defender

If you have integrated Defender for Endpoint with Intune and onboarded your devices, you can also leverage Microsoft Defender for Endpoints **Threat & Vulnerability Management** (**TVM**).

Because you have an Intune device compliance policy to classify devices with a **medium** or **high** level of risk as noncompliant, the compromised device is classified as noncompliant. This happens as service-to-service communication, so it does not rely on Windows when doing an MDM sync as all other settings in the compliance policy do.



NOTE

Do not implement this policy if you have devices running with a threat level that is higher than what you allow in your policy as it will block access right away. Instead, resolve any risk score on your devices before putting this into production.

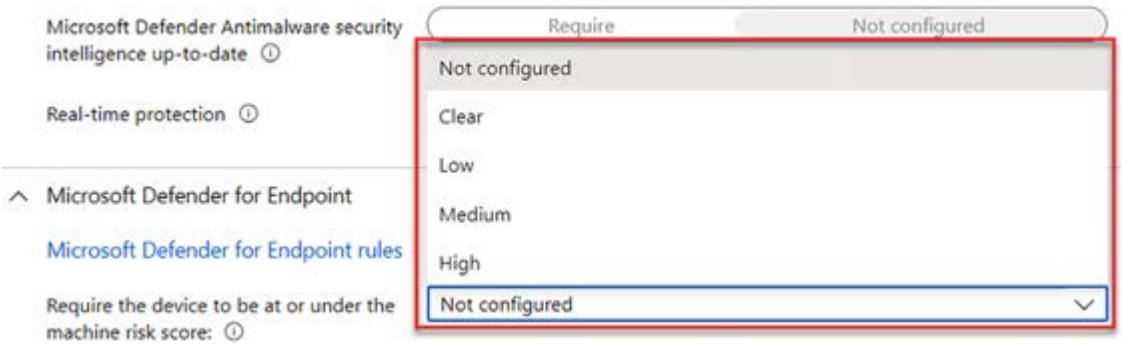


Figure 10.70: Compliance policy – Defender for Endpoint

When you have configured the compliance settings, the next step of the wizard to is configure **Actions for noncompliance** devices. By default, the action is to mark the device noncompliant immediately:

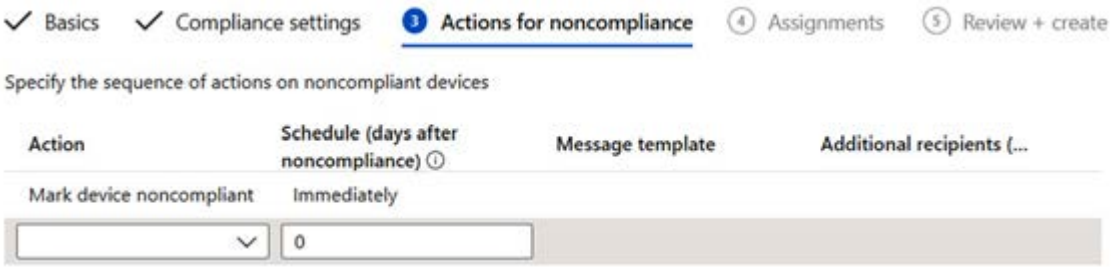


Figure 10.71: Actions for noncompliance

You can also configure **Action for noncompliance** to **Send email to end user** (in the case of the device being noncompliant, the primary user of the device will get an email) or **Add device to retire list**, which is shown in the **Retire noncompliant devices** report under **Devices | Compliance**.

As an IT admin, you can monitor different parts of the compliance state:

- **Compliance Operational report:** Provides real-time operational reports that can help the IT admin take action based on the data they find in this report.

Step 1: Go to **Home** | **Devices** | **Compliance.** Here, you can see an overview of monitoring reports.

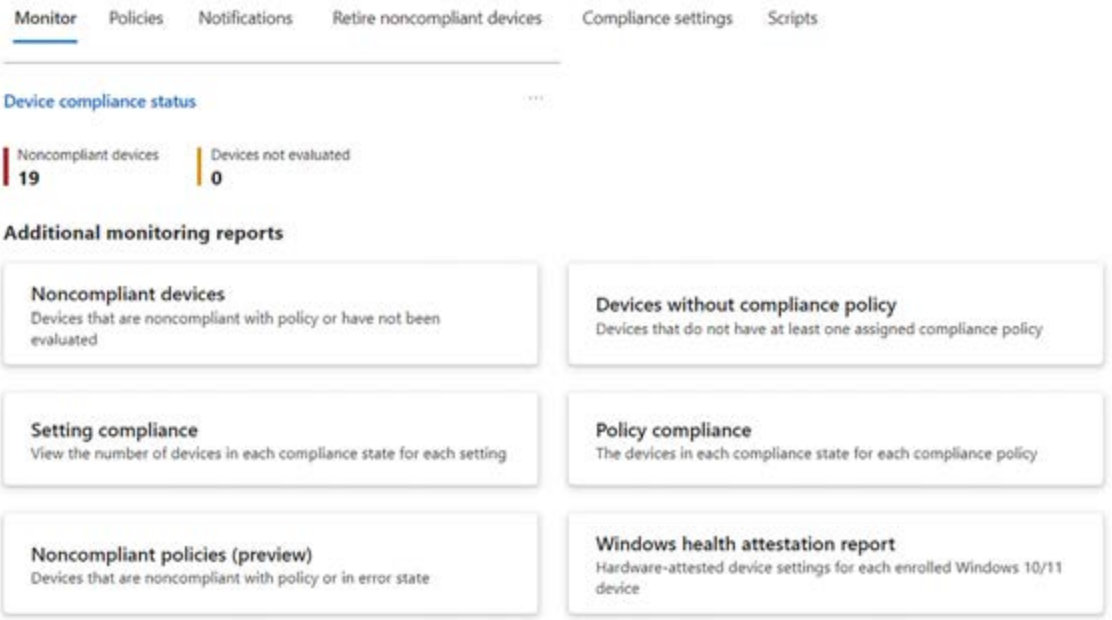


Figure 10.72: Compliance monitoring reports

Step 2: Go to **Home** | **Devices** | **Compliance** | **Monitor** | **Windows health attestation report**. Here, you have the option to see how many of your devices do not have BitLocker and Secure Boot enabled, as an example:

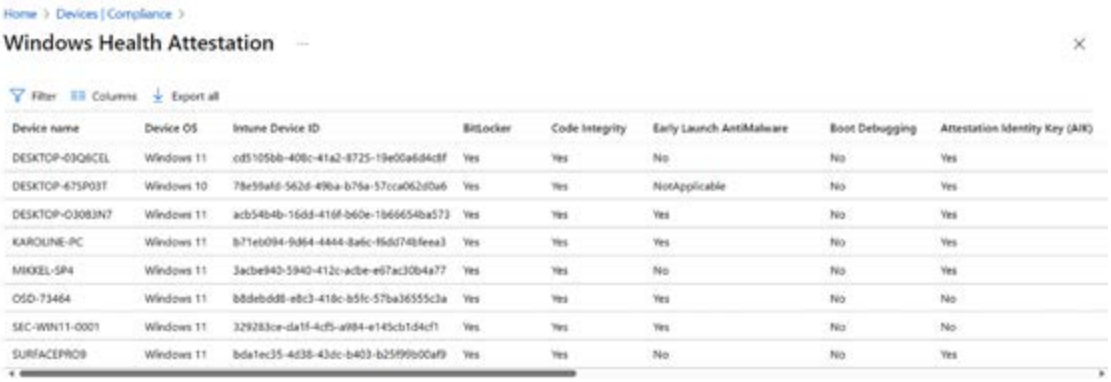


Figure 10.73: Windows health attestation report

- **Noncompliant devices report:** Go to **Home** | **Devices** | **Compliance** | **Monitor** | **Noncompliant devices.**

  In this report, you have the option to see all your noncompliant devices. If you apply the **OS = = Windows** filter, you will only see the noncompliant Windows devices:

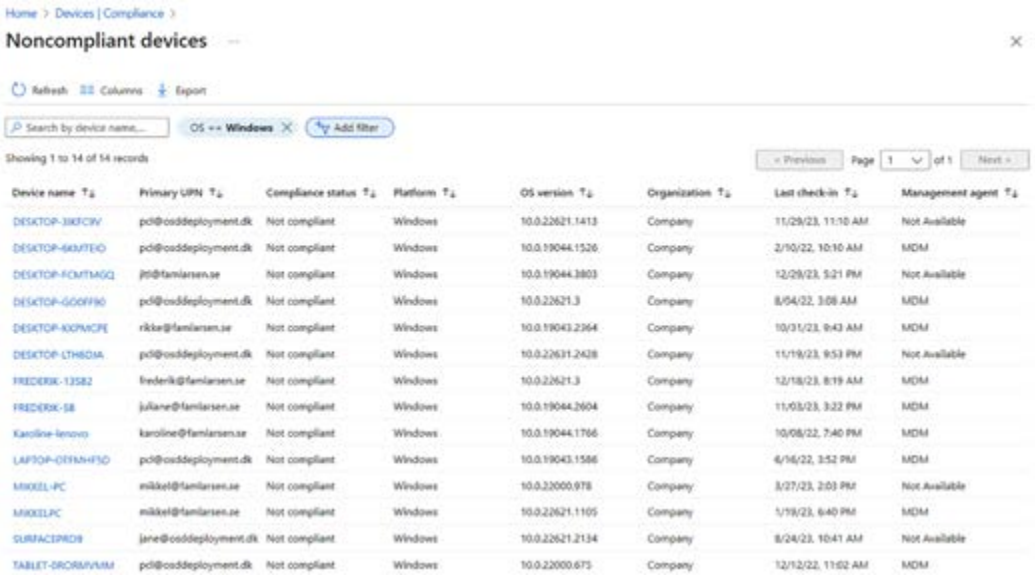


Figure 10.74: Monitor – Noncompliant devices

- **Noncompliant policies (preview)**: Go to **Home** | **Devices** | **Compliance** | **Monitor** | **Noncompliant policies (preview)**.

  In this report, you get a quick overview of your compliance policies in Microsoft Intune and how many devices are not compliant with a specific compliance policy:



Figure 10.75: Monitor – Noncompliant policies (preview)

This concludes this section on compliance policies and how to do operational monitoring of compliance policies. Next, we will cover organizational reporting on compliance.

Organizational compliance report

This is a summary report that gives an overall view of, in this case, the compliance status of your devices. This report gives you a quick overview of the compliance status of all devices in Microsoft Intune.

Go to **Home** | **Reports** | **Device compliance.**

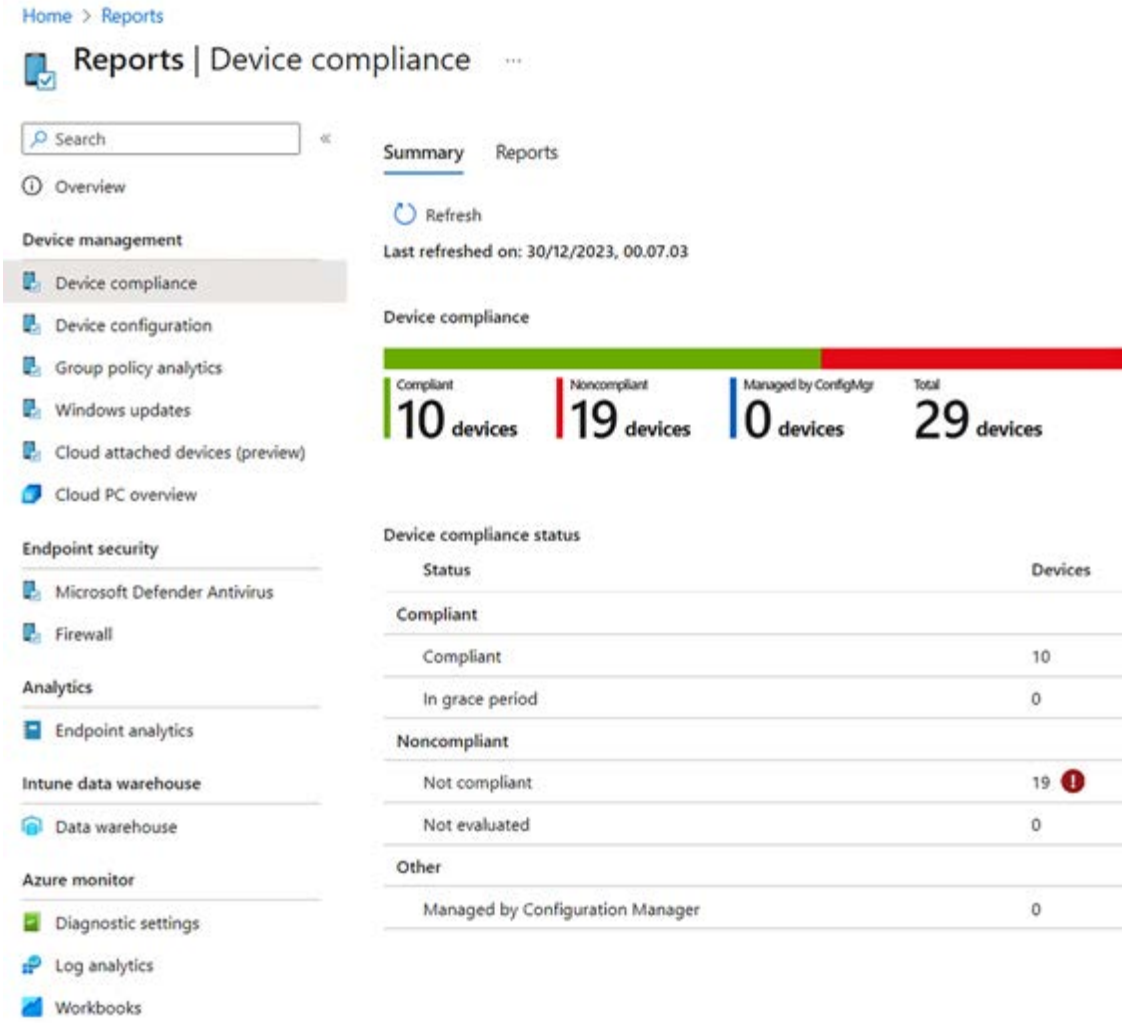


Figure 10.76: Reports – Device compliance – Summary

By clicking on **Reports**, you will get the **Device compliance** and **Device compliance trends** options:

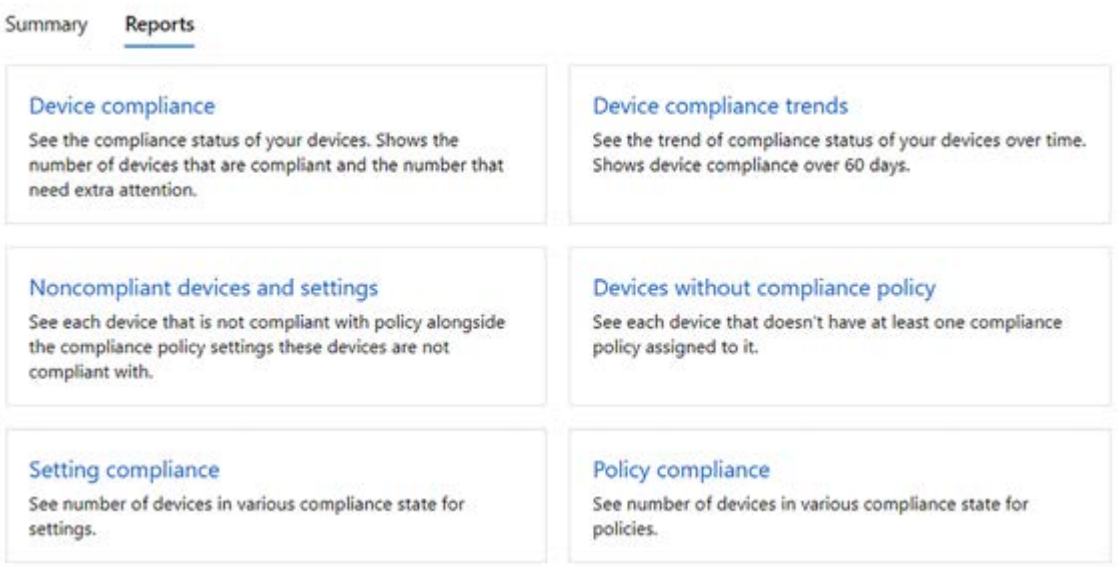


Figure 10.77: Reports – Device compliance

With **Device compliance**, by leveraging the filters, you can select Windows devices and get a report on those devices alone. You can also filter based on the compliance's status and/or ownership:

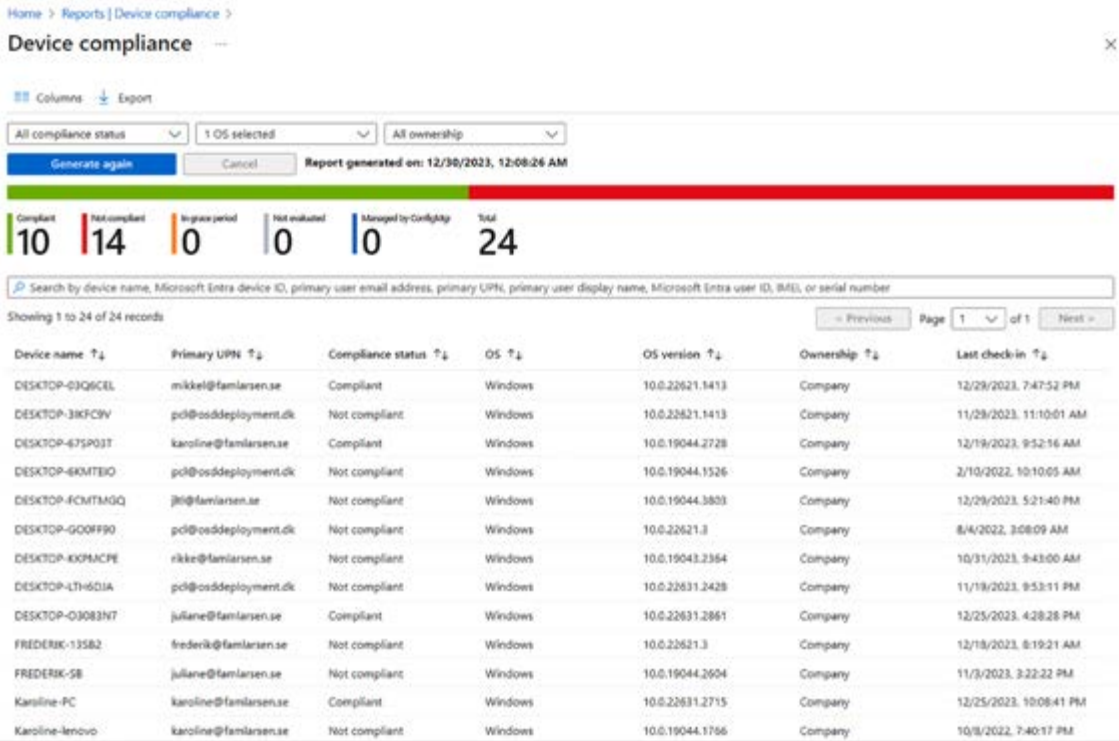


Figure 10.78: Reports – Device compliance

Device compliance trends

This report will provide you with a historical view of your compliance status for the last 30 days. If you need more than 30 days of compliance data, read the next section.

In this view, we have a filter for setting Windows as the OS again:

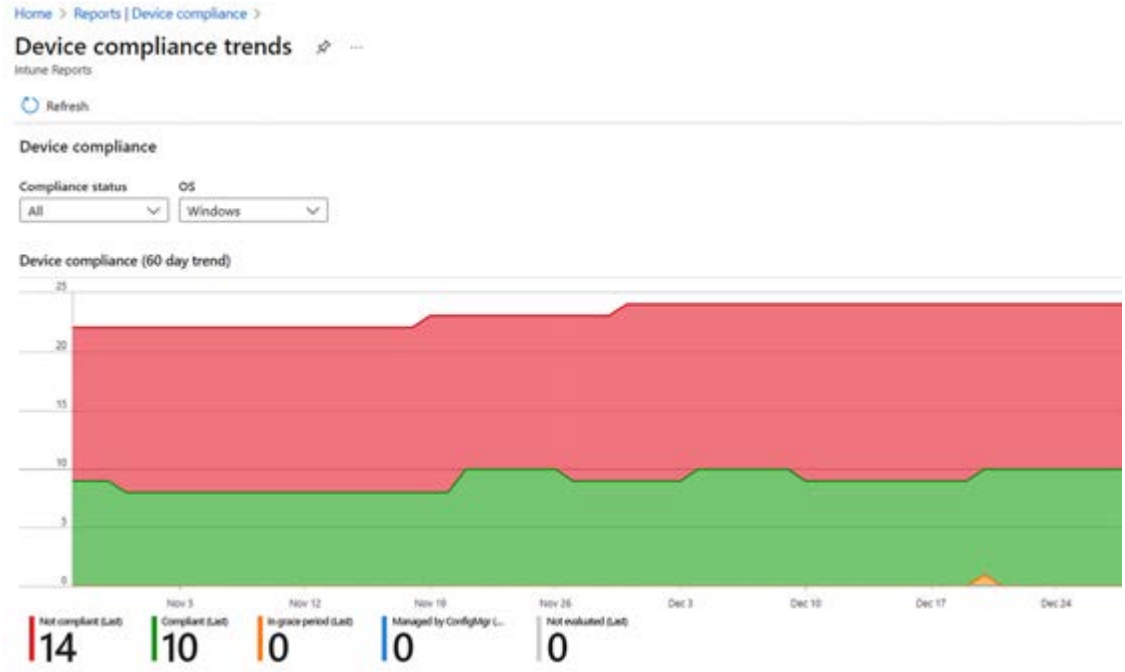


Figure 10.79 – Reports – Device compliance trends

This concludes the section on compliance reporting, In the next section, we will show you how to export Intune compliance data to an external source.

Device diagnostics settings

Diagnostic settings are used to configure the streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations.

Go to the Intune admin center, where you can configure **Diagnostics settings** to export `DeviceComplainceOrg` data to one of the following sources:

- Send to a Log Analytics workspace.
- Archive to a storage account.
- Stream to an event hub.
- Send to a partner solution.

This is not included in your Intune license and can have additional costs for your environment.

You can configure the export by clicking on **Tenant administration | Diagnostics settings | Add diagnostic setting:**

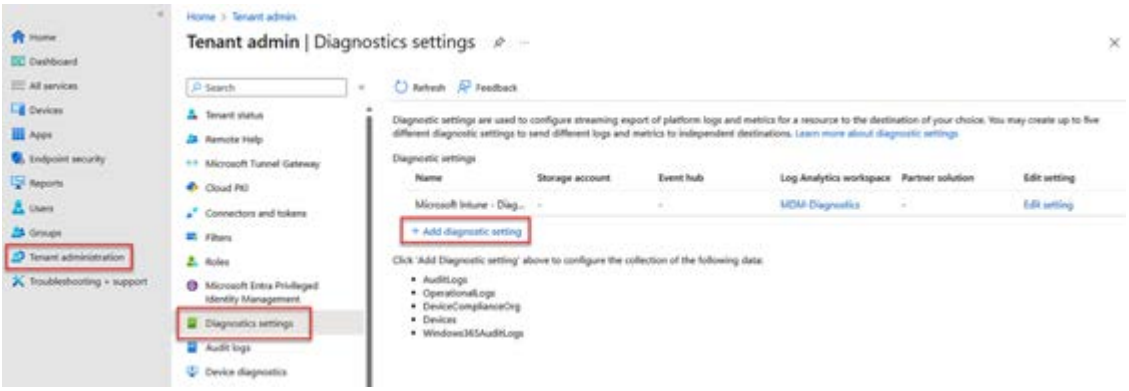


Figure 10.80 – Diagnostics settings

In this example, we will export the data to a Log Analytics workspace:

- Enter **Diagnostic setting name: DeviceComplianceOrg.**
- Select **DeviceComplianceOrg.**
- Select **Send to Log Analytics workspace** and select your Azure subscription and Log Analytics workspace.

You need to have an existing Azure subscription and already have created a Log Analytics workspace to configure this.

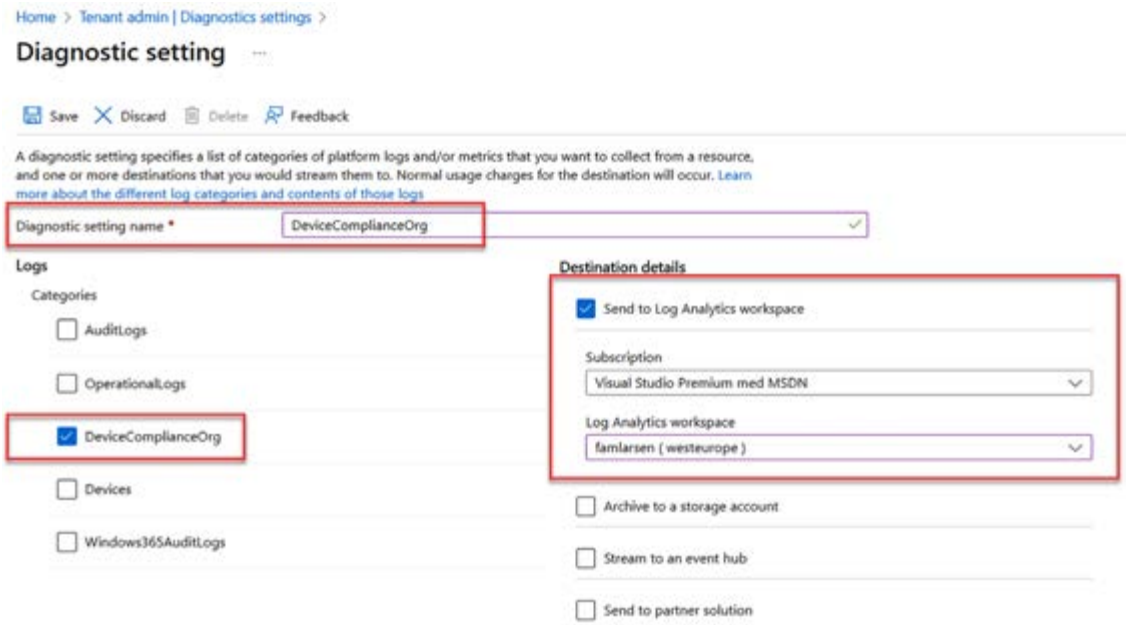


Figure 10.81: Diagnostics settings – Send to Log Analytics workspace

You can export as many of the collection of datasets in one diagnostic setting as you want, but the data can only be exported to one destination per diagnostic setting.

You have the option to export the following collections of data:

- AuditLogs
- OperationalLogs
- DeviceComplianceOrg
- Devices
- Windows365AuditLogs

This concludes this section on how you can export diagnostic settings.

Summary

In this chapter, you've learned about the different policy types and looked at scenarios for configuring Windows in a more modern way via Microsoft Intune for both physical and cloud endpoints. We have looked at some scenarios and policy configurations that you can leverage. In the policy management area, you need to figure out what kind of approach you want to take in your enterprise environment. When looking at pure cloud-managed devices and policies, it would be the perfect time to look forward and not backward. As examples, start by deploying policies that have a positive security impact, such as the Edge security baseline, Windows Defender policies, and so on. Then, look at deploying policies that will help your end users be more productive, such as configuring OneDrive Known Folder Move, policies that help end users start working in their apps better, such as autoconfiguring Microsoft Edge, removing prompts from applications, and so on. After testing with your end users regarding their experience and any feedback they have, you can go back and change your policies to fit the business requirements. The same goes for when you are talking to application owners in your business, or your security department has specific requirements for what certain policies or settings should be on your devices. This is an ongoing process to evaluate whether you are using the correct policies in your environment, just as you probably had a similar process when your policy configuration was done with GPO.

Update the above, you will be able to configure and manage your physical and cloud endpoints. The next chapter is *part three* of **Policy Management** and looks at a cloud service that you can leverage if you have Office 365 to configure Microsoft 365 apps, both with and without Microsoft Intune.

Questions

1. What is DFCI?
    a. A service to optimize the performance of your SSD.
    b. A service with a sense of humor.
    c. Device Firmware Configuration Interface.
    d. A way to configure UEFI on devices that support it.

2. What is the recommended option to start configuring settings on your Windows endpoints?
    a. Settings catalog
    b. Administrative templates
    c. Security baseline
    d. Device restriction profile
3. What policy type can you use to configure Microsoft Edge?
    a. Shared multi-user device
    b. Administrative templates
    c. Kiosk profile
    d. Device restriction profile

Answers

1. (c)
2. (a)
3. (b)

Further reading

If you want to learn more after reading this chapter, please take a look at the following free online resources:

- Device compliance policies in Microsoft Intune – Azure | Microsoft Docs: `https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started`
- Use templates for Windows 10 devices in Microsoft Intune – Azure | Microsoft Docs: `https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows`
- Restrict device features using policies in Microsoft Intune – Azure | Microsoft Docs: `https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-configure`

Join the CloudPro Newsletter with 44000+ Subscribers

Want to know what's happening in cloud computing, DevOps, IT administration, networking, and more? Scan the QR code to subscribe to **CloudPro**, our weekly newsletter for 44,000+ tech professionals who want to stay informed and ahead of the curve.



`https://packt.link/cloudpro`

11

Intune Suite

In this chapter, you'll learn everything you need to know about all the new modules that are part of Microsoft Intune Suite. One of the main questions we will answer is how you can leverage those new features on top of Microsoft Intune to build a more secure and robust Windows platform in your enterprise.

In this chapter, we will cover the following topics:

- What is Intune Suite?
- How to get started – requesting a trial
- Specialty device management
- Endpoint Privilege Management:
- Enterprise Application Management:
- How to install applications
- How to update/do versioning of applications
- Cloud certificate management (Cloud PKI)
- Advanced Endpoint Analytics
- Why Windows 365 and Intune Suite are a great combination

What is Intune Suite?

Microsoft Intune is continually evolving and enhancing, providing IT administrators with more tools to implement the least privilege principle on their managed endpoints. The introduction of the Microsoft Intune Suite has ushered in advanced features that were once only accessible through third-party solutions.

Intune Suite answers many challenges that you, as an IT administrator or manager/CIO, might have, particularly the challenges around remote working and different types of management solutions and devices. The complexity of enterprises is higher than ever before.

The major benefits of Intune Suite are simplification, the ability to reduce IT support costs, and the sunset third-party software that is used as add-ons, to leverage cost-effective Microsoft 365 plans, and decrease surface attacks.



Figure 11.1: Intune Suite benefits

Ok, so what does Intune Suite cover? Let us explain the different components first, and then we will go deeper into the services further in this chapter:

- **Endpoint Privilege Management** (**EPM**): A feature that allows standard users to perform elevations approved by their organization.
- **Enterprise App Management**: A feature that simplifies how organizations package, deploy, and update third-party apps. It is a key addition to Intune Suite.
- **Cloud Certificate Management** (**Cloud PKI**): A cloud-based certificate management solution for secure authentication and Wi-Fi scenarios.
- **Remote Help**: A secure, cloud-based solution for connecting help desk support to end users.
- **Advanced Endpoint Analytics**: A set of analytics-driven capabilities that help IT admins understand, anticipate, and improve the end user experience.
- **Specialized devices management**: A set of device management, configuration, and protection capabilities for special, purpose-built devices such as AR/VR headsets, large smart screen devices, and conference room meeting devices.
- **Tunnel for Mobile Application Management**: A lightweight VPN solution for mobile devices without enrollment.

In this book, we will only cover the Windows-related features of Intune Suite, but several products in Intune Suite already have cross-platform support. A great example is Intune Plan 2, which Android **Firmware Over-the-Air** (**FOTA**) is available for. FOTA updates allow you to remotely update the firmware of supported devices wirelessly with more control. Currently, Zebra and Samsung devices are supported.

Prerequisites

To use Intune Suite, you would need to be licensed for Microsoft Intune Plan 1 from existing Enterprise Mobility + Security E3/E5, or Microsoft 365 E3/E5, F3/F5, or Business Premium plans.

The table below will help explain the various options per service in a more simplified way.

Services	Intune Plan 1	Intune Plan 2	Intune Suite
Intune Core Capabilities	Included	Included	Included
EPM	Add-on	Add-on	Included
Enterprise App Management	Add-on	Add-on	Included
Cloud Certificate Management (Cloud PKI)	Add-on	Add-on	Included
Remote Help	Add-on	Add-on	Included
Advanced Endpoint Analytics	Add-on	Add-on	Included
Specialty Device Management		Included	Included
Tunnel for Mobile Application Management		Included	Included

Table 11.1: Intune Suite

How to get started with Intune Suite

If you want to kick the tires and try things out in your own tenant, you can use the free trial, which gives you a 90-day period to use the Intune add-on capability without any charge. Trials can be applied to up to 250 users per tenant. At the end of the trial period, there's a 30-day grace period. After this point, you'll be unable to use the Intune add-on capability in Microsoft Intune for users within your tenant unless you've purchased the appropriate licenses. There's a one-time limit to start a trial for each tenant.

If you want to test out EPM, as one example, we recommend that you enable a separate EPM trial license, as a trial license can only be activated once per tenant. This means if, at a later point in time, you want to try another product, you can still enable the Intune Suite trial in your tenant as it has not been activated before.

Purchasing licenses lets you use the Intune add-on capability in your tenant for the duration in which the licenses are active on your tenant based on the option selected during the billing process.

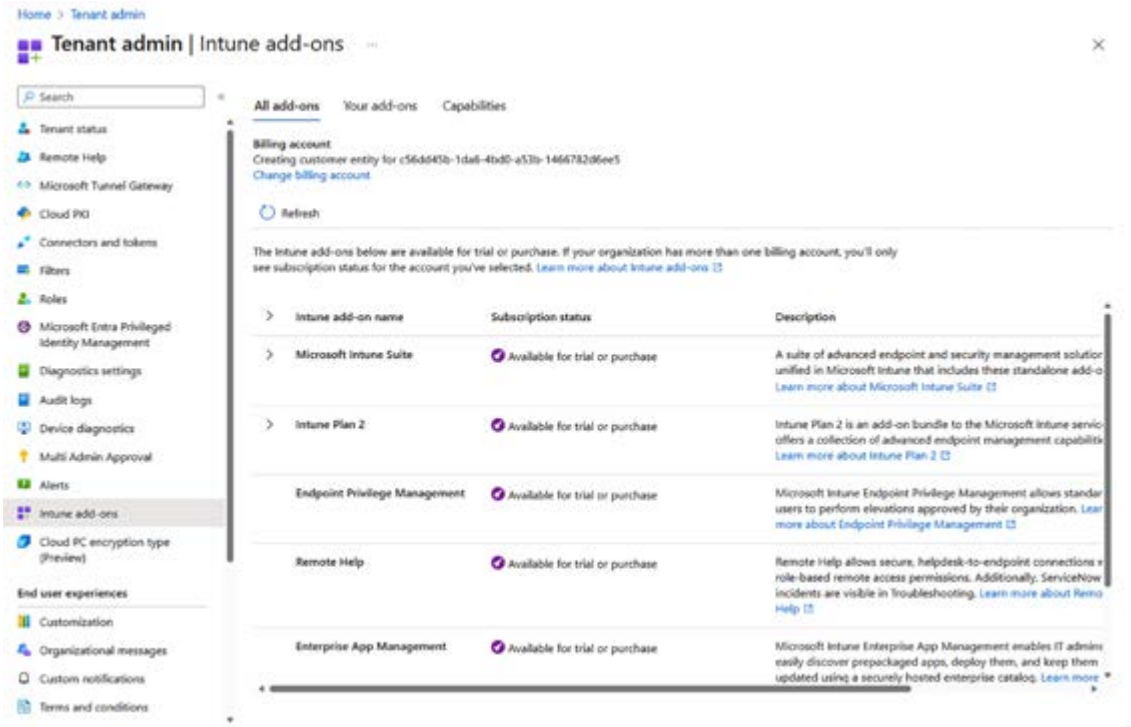


Figure 11.2: Intune add-ons

You can request a trial for Intune Suite at the Microsoft 365 admin center portal via `https://admin.microsoft.com/`.

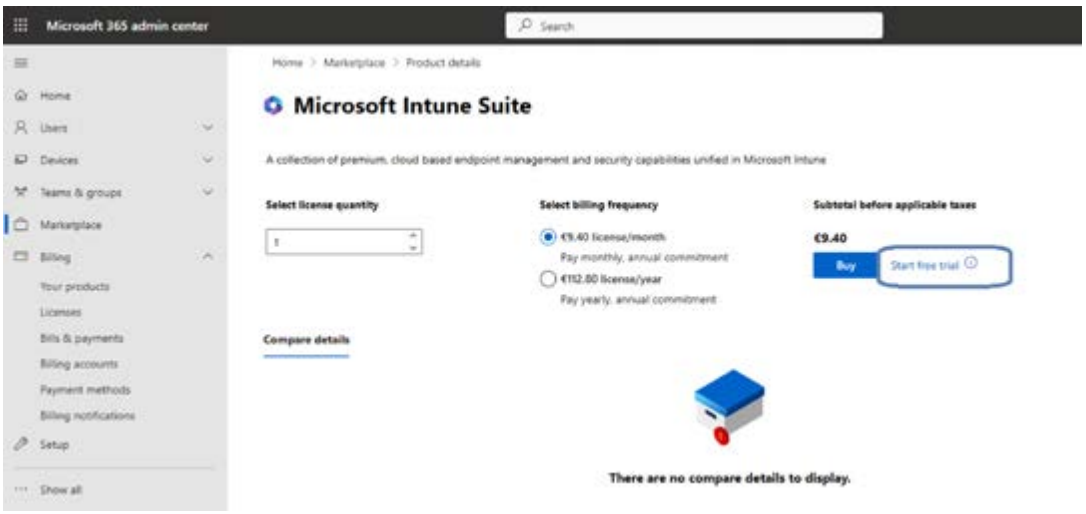


Figure 11.3: Intune Suite trial

Ensure that you assign the licenses to your users afterward via either direct-to-user attachment or creating an Entra ID group that automatically assigns the licenses to your users.

Specialty Device Management

Specialty devices can be AR/VR devices, HoloLens, RealWear, HTC, Team Rooms systems, and other types of devices running both Windows and Android.

For Microsoft Teams Rooms devices, including Surface Hub, you are properly licensed with a Teams license that includes Intune management.

For Microsoft HoloLens, subscribers of Microsoft Intune (Plan 1) aren't required to proactively add the Intune Plan 2 license to their tenant. You can keep managing it, as done previously, as an interim solution until Microsoft has found a solution to integrate it as part of the Microsoft subscriptions.

As for any other licenses, always have a conversation with your licensing partner so that you can ensure that you are license-compliant.

Endpoint Privileged Management

Endpoint Privilege Management (**EPM**) supports your zero-trust journey by enabling your organization to establish a broad user base operating with minimal privileges, while still permitting users to execute tasks authorized by your organization, thus maintaining productivity. The key features of EPM are:

- Automatic, user-confirmed, or support-approved elevation
- Insights based on elevation audits
- Effective control of child processes
- Rules based on organizational requirements
- Easy addition or removal of rules
- Tenant-level enablement per device rollout

How to configure EPM

EPM is a feature that allows users to run as a standard user (without administrator rights) and complete tasks that require elevated privileges.

To configure EPM, you need to have the following prerequisites:

- Microsoft Intune Plan 1 license
- Microsoft Entra joined or Microsoft Entra hybrid joined
- Microsoft Intune Managed, either as cloud-native or as Configuration Manager co-managed (no workload needs to be shifted to Intune)
- A clear line of sight to the backend service (SSL inspection is not supported with EPM)

Once you have all the prerequisites, you can configure EPM in the Microsoft Intune admin center. The configuration process involves the following steps:

1. Create a list of applications that need elevated privileged access to run. This step is a recurring step to keep the list up to date.
2. Create an onboarding and default elevation setting policy.
3. Create policies to manage how a file elevation request is handled.
4. Check the EPM reports for unsuccessful elevation requests and then restart at *step 1*.

How to onboard devices to EPM

First, you need to create an Endpoint Privilege Management elevation setting policy that also starts onboarding the devices into EPM as you have assigned the policy.

To configure the elevation setting policy, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Endpoint Security** | **Endpoint Privilege Management** | **Create Policy**:
    - **Platform**: Select **Windows 10 and later**
    - **Profile**: Select **Elevation setting policy**

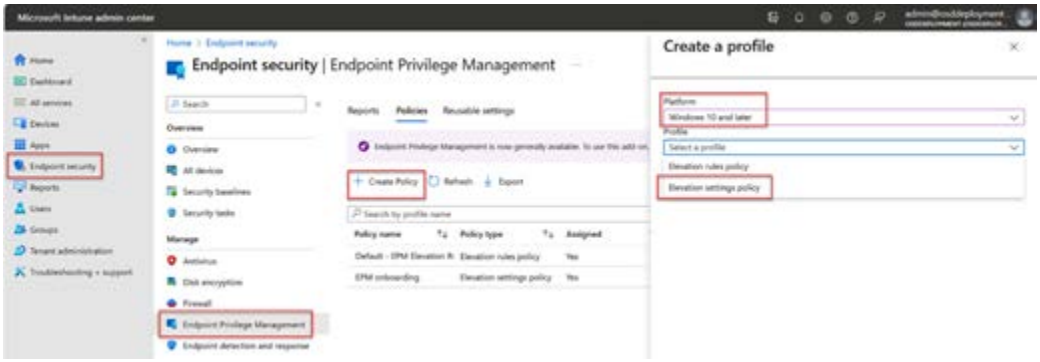


Figure 11.4: EPM Elevation settings policy

2. Enter a name for the policy. It is optional to add a description.

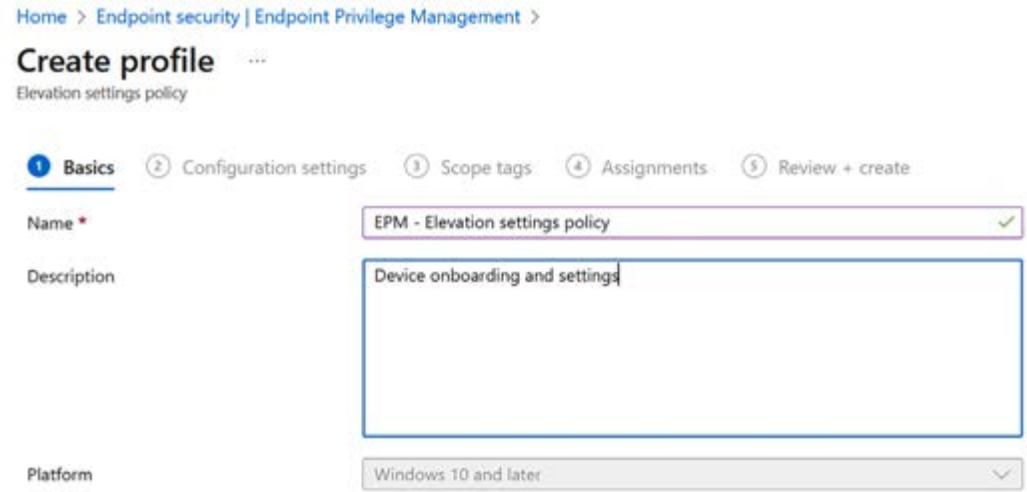


Figure 11.5: EPM Elevation Settings policy, Basics

3. In **Configuration settings**, choose **Enabled** for the Endpoint Privilege Management toggle.

   This policy is what starts the device onboarding process into EPM and provisions the binaries that are used on the Windows client.

If this policy setting is set to **Disabled** at a later point, then it will make the EPM client components dormant on targeted devices. After 7 days, the EPM components will be removed from the Windows client – this is by design in case you disable the policy by mistake. The EPM binaries will not need to be pushed to the Windows client again if the policy setting is flipped back to Enabled within those first 7 days. You will see the same behavior if the policy is unassigned – unassigning also means changes within nested groups, which is a case we often see when troubleshooting.

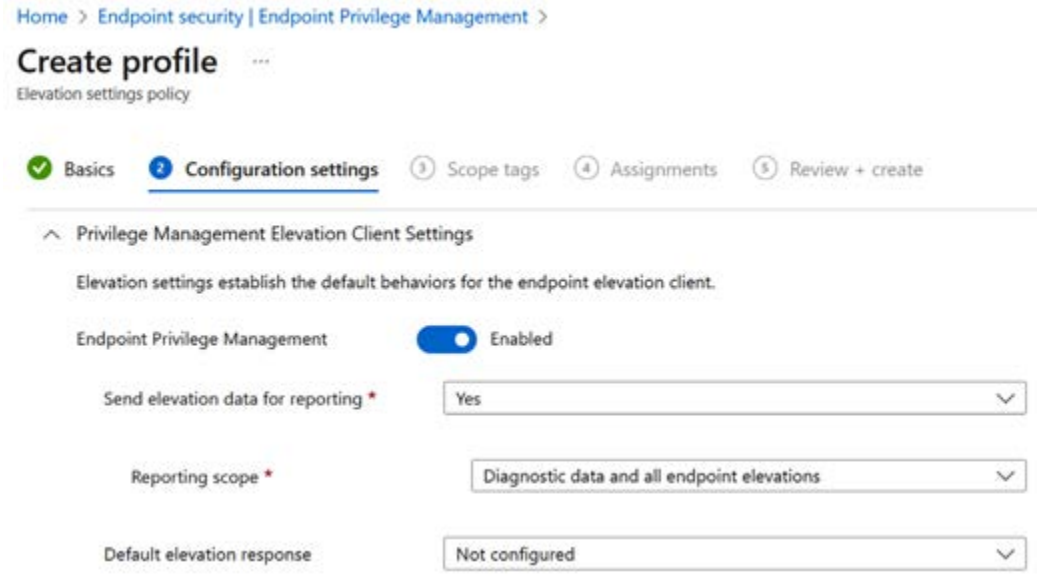


Figure 11.6: EPM Elevation settings policy, Configuration settings

4. For **Send elevation data for reporting**, select **Yes.**

   Yes is the default option, which allows the client to send elevation data to Microsoft and have it show up in your EPM report in your Microsoft Intune tenant.

   If it is configured to **No**, elevation data will not be sent to Microsoft and you will not see any data in your EPM reports.



Figure 11.7: Send elevation data for reporting

5. **Reporting scope** is where you configure what kind of data will be sent and available in your EPM reports.

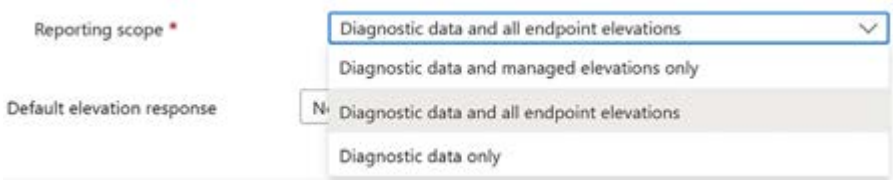


Figure 11.8: Reporting scope

6. From the three options available, we will recommend **Diagnostic data and all endpoint elevations** so you have as much visibility as possible in your EPM reports. These are the three options:

   - **Diagnostic data and managed elevations only** – Sends diagnostic data to Microsoft about the health of the EPM client components and data about elevations being facilitated by EPM.
   - **Diagnostic data and all endpoint elevations** – Sends diagnostic data to Microsoft about the health of the EPM client components and data about all elevations happening on the endpoint.
   - **Diagnostic data only** – Sends diagnostic data to Microsoft about the health of the EPM client components only.

   Diagnostic data is used by Microsoft to measure the health of the EPM client components. If you have chosen one of the options with elevation data, that data will show up in the EPM report; the data shown in the reports can easily be used to create elevation rules in your environment.

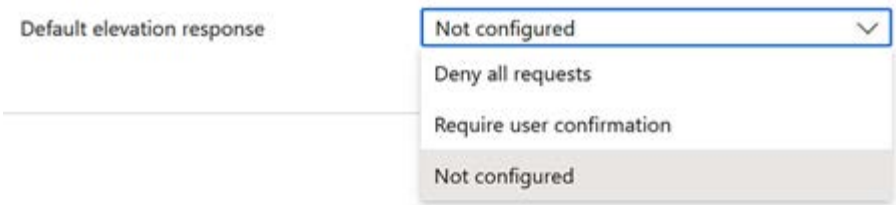


Figure 11.9: Default elevation response

7. **Default elevation response**: The most secure option here is to select **Deny all requests**, which requires the IT admin to create specific rules for executables on the devices that are allowed to run with elevated privileges.

   Let's look at all three options:

   - **Deny all requests** – This is the strictest option as it blocks all elevate requests that are not defined in an elevation rules policy.
   - **Not configured** – This will enable EPM in an "audit" mode where you will be able to collect data on elevations; this will show up in the EPM elevation report as unmanaged actions.

- **Require user confirmation** – When user confirmation is required, you can choose from the same validation options.

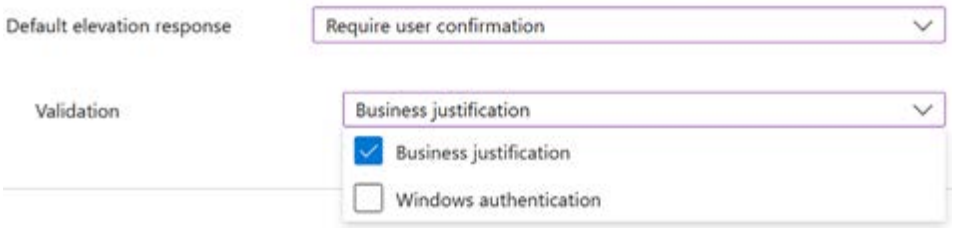


Figure 11.10: Default elevation response validation

8. You get the option to set a **Validation** option when you select **Require user confirmation** in the **Default elevation response** setting:
    - **Business justification** – This will require the end user to provide a business justification in clear text before completing the elevation. The business justification will be visible to the IT admin in the EPM report.
    - **Windows authentication** – This will require the end user to authenticate before completing an elevation, which means that any Windows authentication is valid, including Windows Hello for Business authentication.
9. Now, you just need to assign it to a group of users or devices. That will start the onboarding process into the EPM backend service.

Reusable settings

Before we dig into how to create an EPM policy, we need to cover reusable settings as they can help you as an IT admin, and make it easier for you to create policies.

Reusable settings are not only for EPM but also applicable to firewall and **Azure Site Recovery** (**ASR**) policies, which we covered in *Chapter 10*, *Advanced Policy Management*.

Reusable settings for EPM allow you to reuse the same certificate when you create multiple EPM policies. For example, we will walk you through how to add the Adobe Inc. code-signing certificate that is used on its installers, such as Adobe Reader:

1. First, you need to download the latest Adobe Reader as an executable, enter the properties of the file, and then click on **Digital Signatures**.

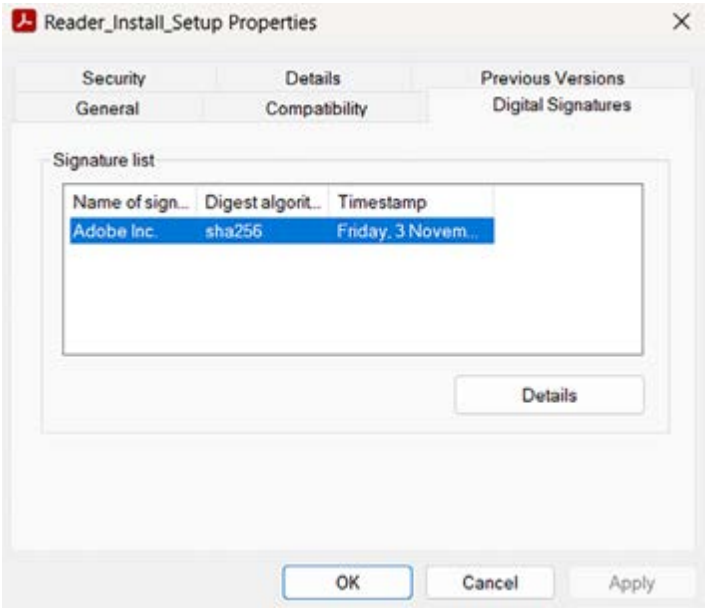


Figure 11.11: Adobe Reader installation details

2. Click **Details** for the Adobe Inc. certificate, as shown in the preceding figure.

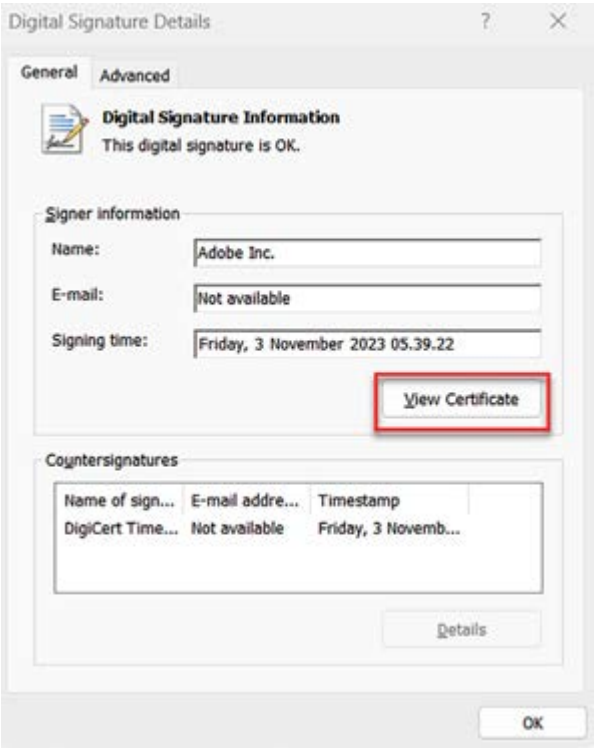


Figure 11.12: Adobe Inc. View Certificate

3. Then, you need to click on **View Certificate**, as shown in the preceding figure.

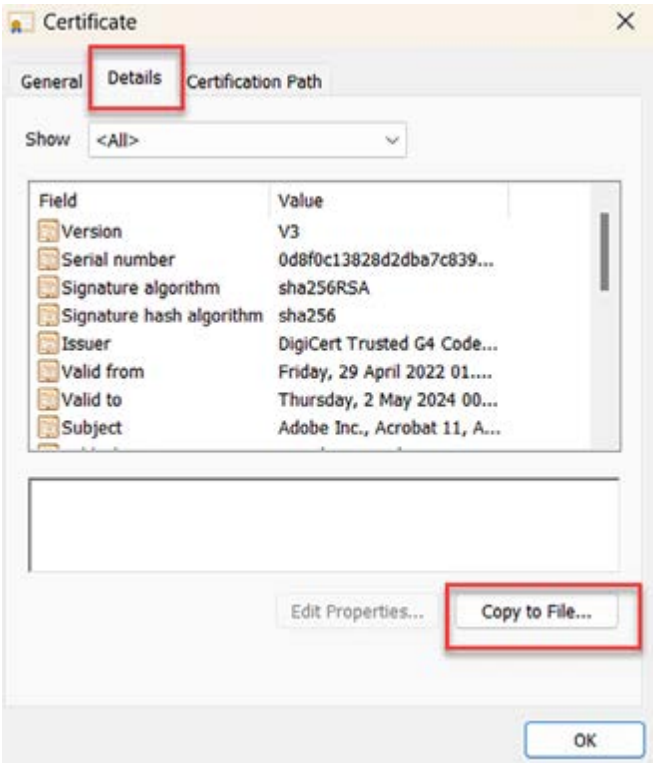


Figure 11.13: Adobe Inc. Copy to File

4. Click **Details** and then click on **Copy to File**, as shown in the preceding figure.
5. Continue to the Certificate Export Wizard by clicking **Next**.



Figure 11.14: Certificate Export Wizard

6. Then, click **Next** again.

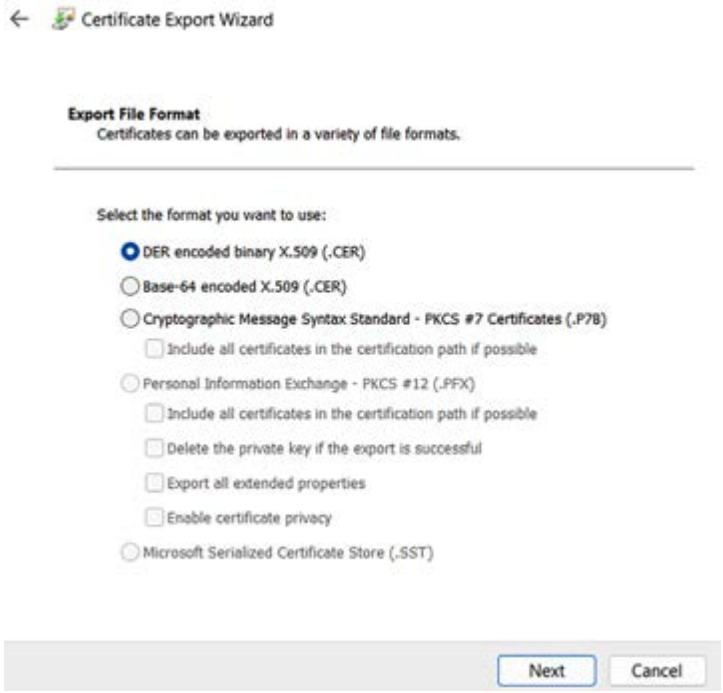


Figure 11.15: Certificate Export Wizard DER .CER

7. Enter the file name **Adobe.cer** and click **Next.**

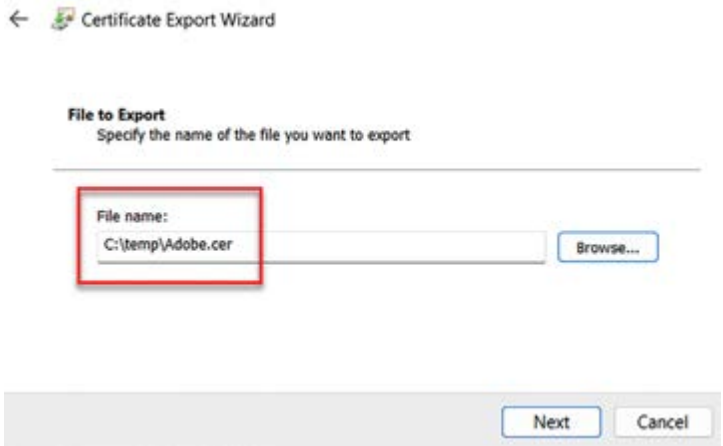


Figure 11.16: Certificate Export Wizard File to Export

8. Click **Finish**, and you are ready to leverage the Adobe Inc. code-signing certificate in an EPM reusable settings policy.

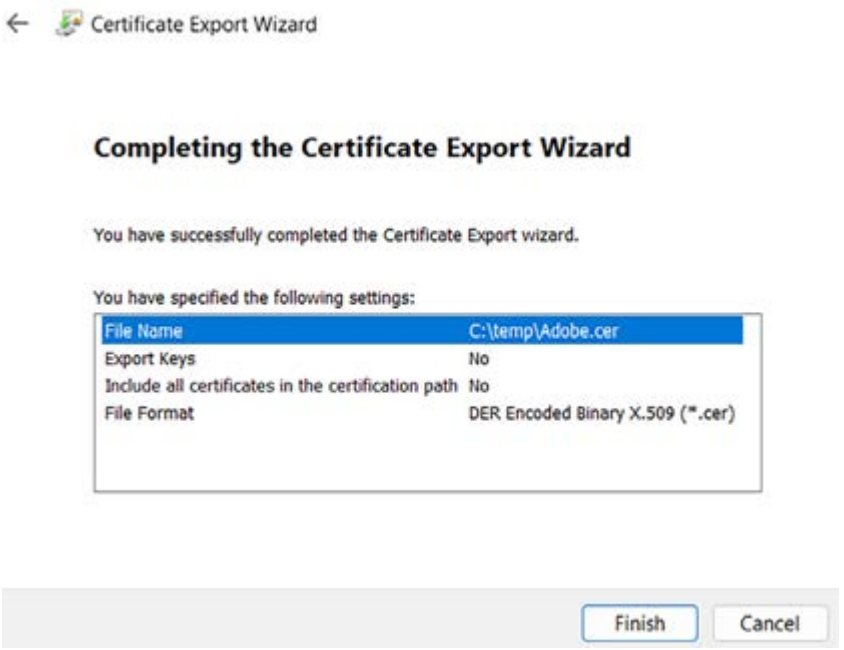


Figure 11.17: Certificate Export Wizard Finish

To configure the reusable settings, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Endpoint Security** | **Endpoint Privilege Management** | **Reusable settings** | **Add**.
2. Give the reusable settings a name, like `Reusable settings - Adobe Inc`.

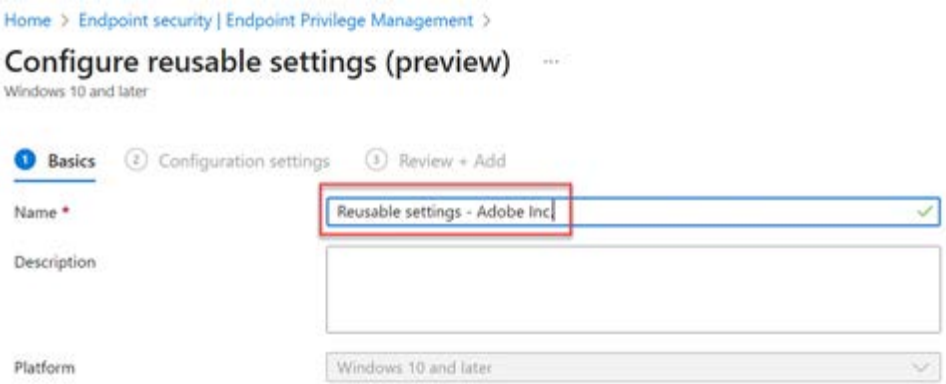


Figure 11.18: EPM reusable settings, Basics

3. Browse for the coding certificate that you just exported.

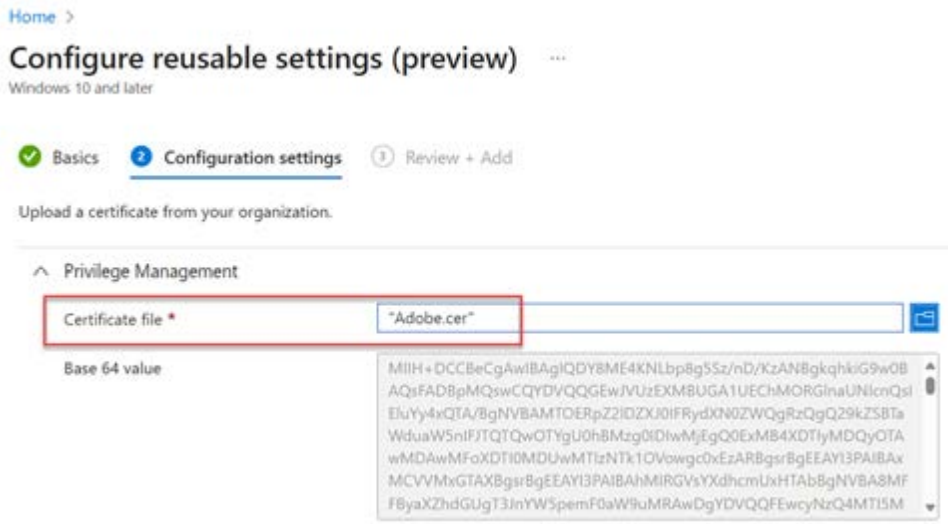


Figure 11.19: EPM reusable settings, Configuration settings

Reusable settings cannot be assigned to a group of their own but can be reused in a policy, which we will show you how to create in the next section.

Creating an EPM elevation rules policy

EPM policies are used to whitelist what your end users can run with elevated privileges.

When you create rules, you set the conditions for allowing just-in-time access to apps and files on Windows endpoints and assign the policy to groups of users or devices.

EPM policies need to be kept updated when your applications are updated or you get new applications in your environment that require running with elevated privileges.

To configure the elevation rules policy, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Endpoint Security** | **Endpoint Privilege Management** | **Create profile:**
    - **Platform:** Select **Windows 10 and later**

- **Profile:** Select **Elevation rules policy**

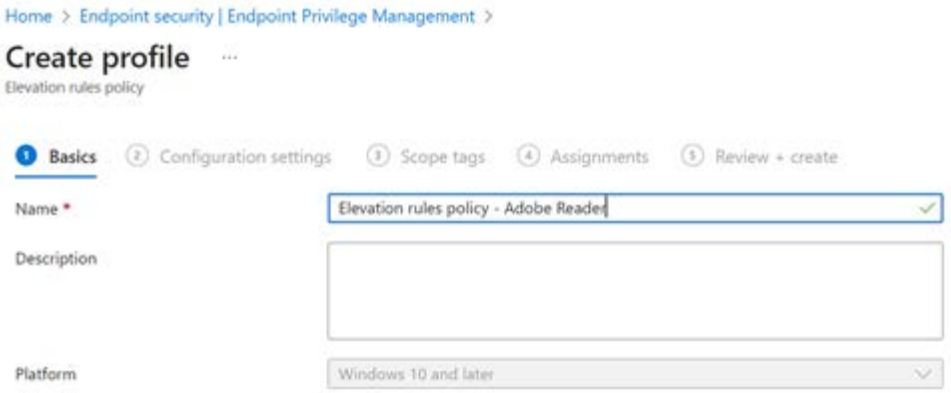


Figure 11.20: EPM Elevation rules policy, Basics

2. You can create as many rules as you want in one elevation rules policy, but first, you need to click **Edit instance** and tick the checkbox for the **User confirmed.**

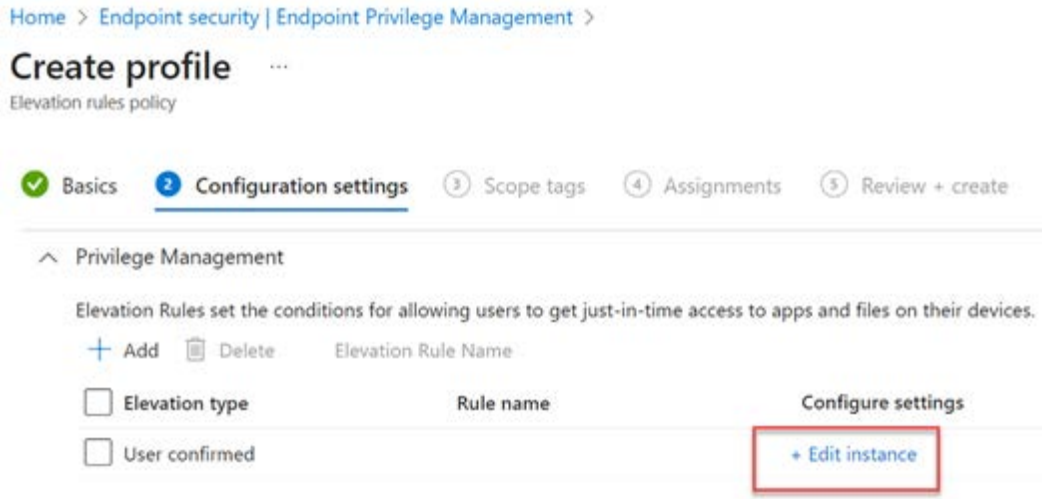


Figure 11.21: EPM Elevation rules policy, Configuration settings

When you have clicked **Edit instance**, you will get the **Rule properties** blade, where you can fill out the details of the executable.

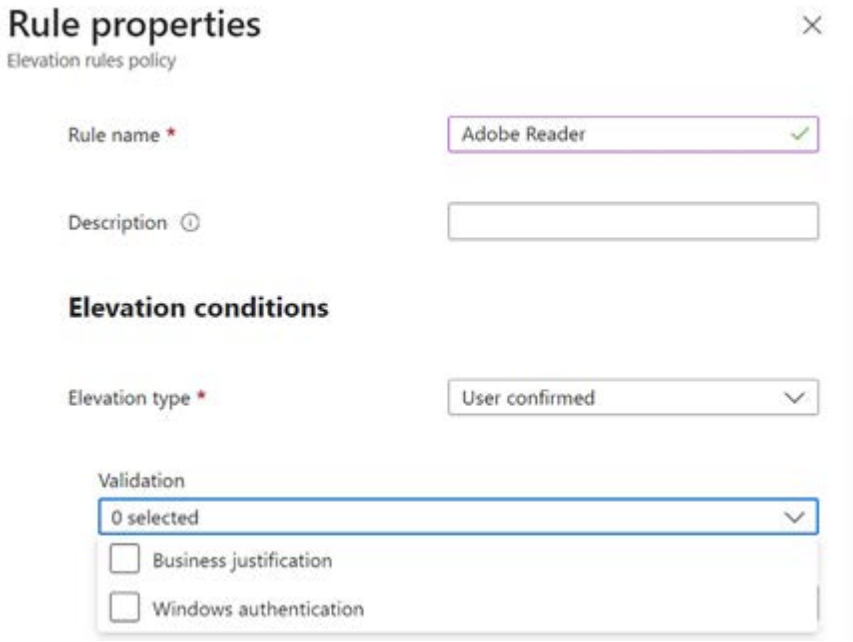


Figure 11.22: EPM Elevation rules policy, Rule name

3. Enter the **Rule name** – in this case, **Adobe Reader**.
4. Select the **Elevation type** – in this example, we selected **User confirmed** so the end user needs to right-click and select **Run with elevated access**.
5. Instead of **User confirmed** as the elevation type, you can select **Automatic**, which does not require any end user interaction to elevate the executable.



Figure 11.23: EPM Elevation rules policy, Child process behavior

6. Let's look at the options in **Child process behavior**:
    - **Require rule to elevate** – Configure a child process to require its own rule before that child process can run in an elevated context.
    - **Deny all** – All child processes launch without elevated context.
    - **Allow all child processes to run elevated** – Configure a child process to always run elevated.
    - **Not configured** – The Windows default.



NOTE

Windows automatically delegates the context of a parent to a child, so take special care in controlling the behavior of your allowed applications. Ensure that you evaluate what is needed when you create elevation rules and implement the principle of least privilege.

7. The most secure option is to deny all child process behavior, which is the recommended option, but some applications call child process that also needs to run elevated.
8. As you continue filling out the rule properties, you will come to the **File information** section.

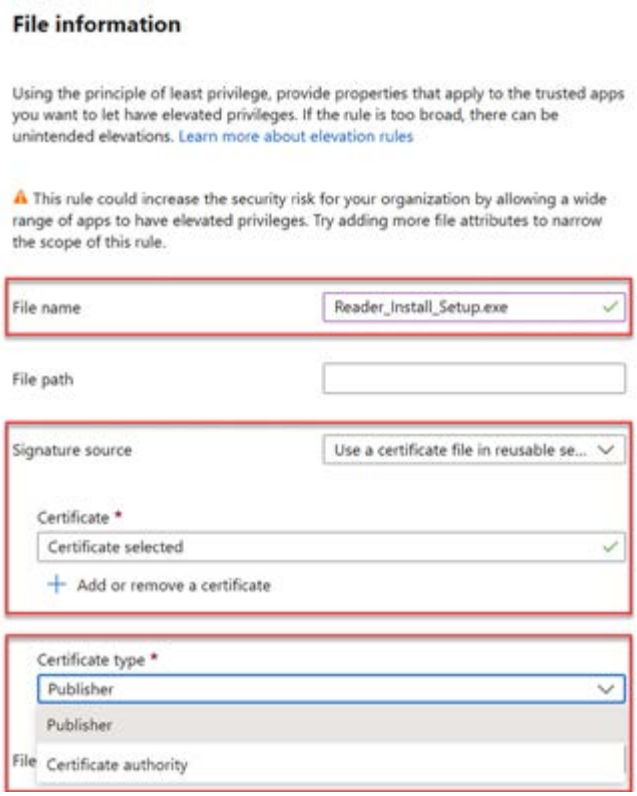


Figure 11.24: EPM Elevation rules policy, File information

9. Here, you can see the policy is issuing a warning, as the policy needs to be more specific to be sure that you are only allowing the binaries to run that you allow. The first step is to add the **File hash** value.



Figure 11.25: EPM Elevation rules policy, File hash

This concludes how to create an EPM elevation rules policy, and you can now deploy it to a group of users or devices. Next, we will show you how to gather the file information you need to build your rules.

As an IT administrator, you can extract the **File hash** value by running a PowerShell `cmdlet`:

1. Open PowerShell as an administrator and run the `get-filehash` `cmdlet` to get the hash value from the file.

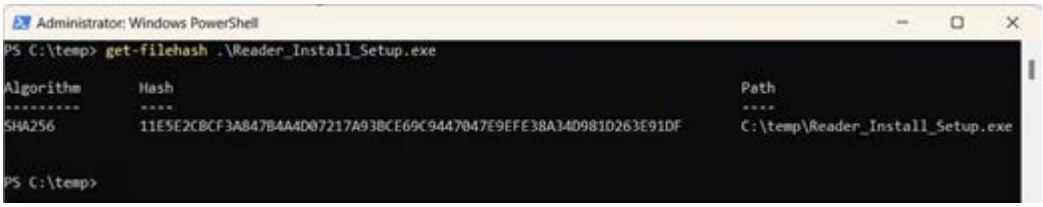


Figure 11.26: get-filehash

When you have the EPM Agent installed on one of your devices, you will have access to EPMTools. By installing this tool, you can get all the file attributes that you can put into an EPM rules policy. Now, we will show how to get access to the tool:

2. First, you need to import the PowerShell module from EPMTools by running this command:

```
Import-Module "C:\Program Files\Microsoft EPM Agent\EpmTools\EpmCmdlets.
dll"
```

3. After you have imported the module, you can run the following:

```
Get-FileAttributes -FilePath "C:\\Temp\\Reader_Install_Setup.exe"
```

4. You will get this result:

```
FileName      : Reader_Install_Setup.exeFilePath      : C:\Temp
FileHash      :
11E5E2CBCF3A847B4A4D07217A93BCE69C9447047E9EFE38A34D981D263E91DF
HashAlgorithm : Sha256
ProductName   : Adobe Download Manager
InternalName  : Adobe Download Manager
Version       : 2.0.0.720
Description   : Adobe Download Manager
CompanyName   : Adobe Inc
```

When you have imported the PowerShell module `C:\Program Files\Microsoft EPM Agent\EpmTools\EpmCmdlets.dll`, you get some additional PowerShell cmdlets that can help you diagnose and perform troubleshooting on the EPM Agent.

Here are some `cmdlets` for elevation rules policies received on the Windows client:

- **Get-Policies:** Retrieves a list of all policies received by the EPM Agent for a given PolicyType (ElevationRules, ClientSettings, etc.). In the following, we give examples of all currently supported parameters:
    - **Get-Policies - PolicyType ElevationRules - Verbose | Format-Table - AutoSize**

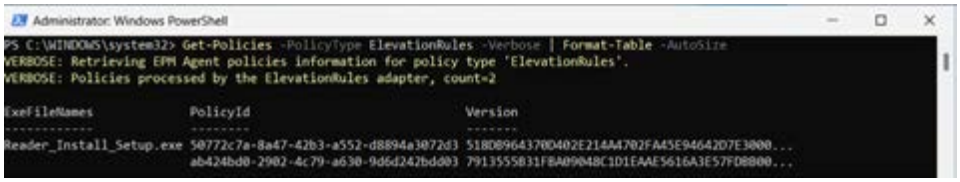


Figure 11.27: Get-Policies ElevationRules

    - **Get-Policies - PolicyType ClientSettings - Verbose | Format-Table - AutoSize**

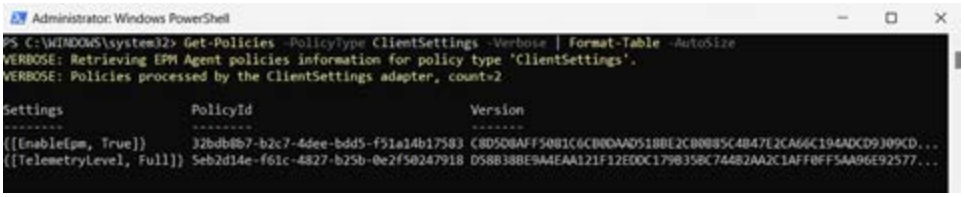


Figure 11.28: Get-Policies ClientSettings

Here are some `cmdlets` for client settings policies received:

- **Get-DeclaredConfiguration:** Retrieves a list of WinDC documents received by DeclaredConfiguration targeting a given PolicyType (ElevationRules, ClientSettings, etc.). These are the policies targeted to the device; for every policy, two WinDC documents are received in the device: one of type MSFTPolicies (actual policy) and one of type MSFTInventory (inventory operation):

- **Get-DeclaredConfiguration - PolicyType ElevationRules - Verbose | Format-Table - AutoSize**



Figure 11.29: Get-DeclaredConfiguration ElevationRules

- **Get-DeclaredConfiguration - PolicyType ClientSettings - Verbose | Format-Table - AutoSize**

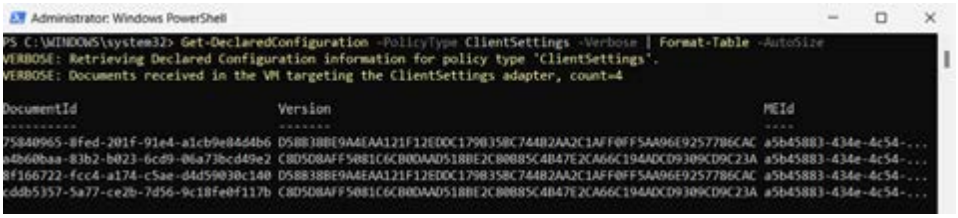


Figure 11.30: Get-DeclaredConfiguration ClientSettings

Here are some `cmdlets` for the WinDC documents received by declared configuration:

- **Get-DeclaredConfigurationAnalysis:** Retrieves a list of WinDC documents of type MSFTPolicies and checks if the policy is already present in the EPM Agent (the Processed column):
  - **Get-DeclaredConfigurationAnalysis - PolicyType ElevationRules -Verbose | Format-Table - AutoSize**

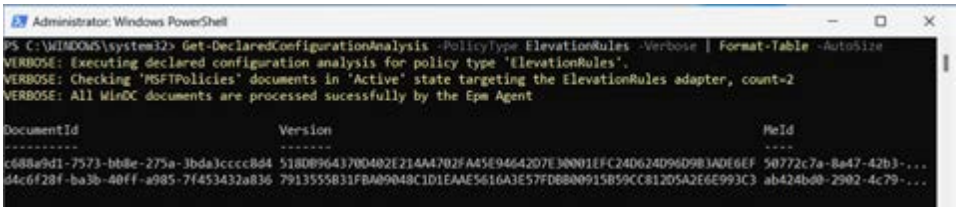


Figure 11.31: EPM Get-DeclaredConfigurationAnalysis ElevationRules

- **Get-DeclaredConfigurationAnalysis - PolicyType ClientSettings - Verbose | Format-Table - AutoSize**

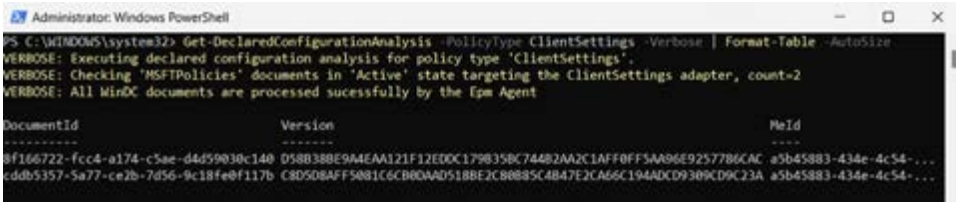


Figure 11.32: EPM Get- DeclaredConfigurationAnalysis ClientSettings

Here are some cmdlets for WinDC documents that are processed by the EPM Agent:

- **Get-ElevationRules:** Queries the EPM Agent lookup functionality and retrieves rules given the lookup and target. Currently, two kinds of lookups are supported (FileName and CertificatePayload):
    - **Get-ElevationRules - Target E98542FE3033531008248C7573DEA139F34FE39C898BF-889CCD9D9C2DDD3C678 -Lookup CertificatePayload - Verbose**



Figure 11.33: EPM Get-ElevationRules -Target CertificatePayload

    - **Get-ElevationRules - Target Reader_Install_Setup. Exe - Lookup FileName - Verbose**

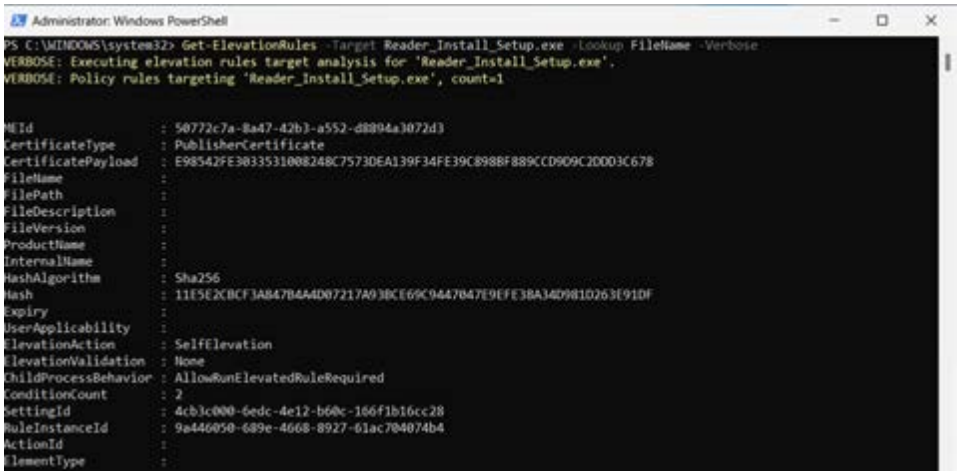


Figure 11.34: EPM Get-ElevationRules -Target FileName

Here are some `cmdlets` for EPM client settings:

- **Get-ClientSettings:** Processes all existing client settings policies, analyzes conflicts (multiple policies with different values for the same setting), and uses hardcoded defaults if needed for policies not present or in conflict, resulting in displaying the effective client settings used by the EPM Agent:
    - **Get-ClientSettings - Verbose**

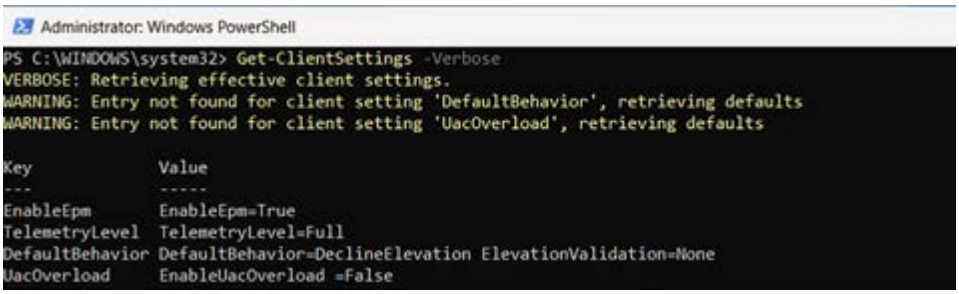


Figure 11.35: EPM Get-ClientSettings -Verbose

Monitoring EPM events

With the built-in reports for EPM, you, as an IT admin, can monitor both the managed and unmanaged elevations on the devices that are onboarded to EPM.

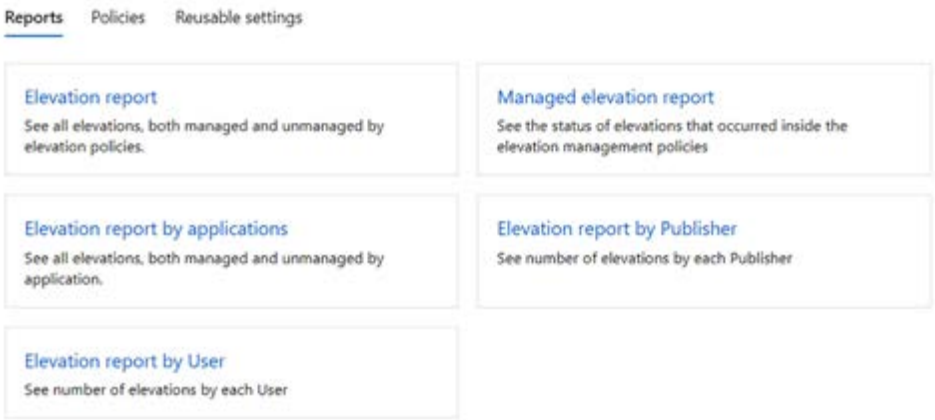


Figure 11.36: EPM reports

As shown in *Figure 11.36*, you can see the different types of reports. Next, we will walk through what you can leverage each of them for.

Elevation report

Using this report, you can see all elevations, both managed and unmanaged by elevation policies.

You can also leverage this report to create an EPM rules policy afterward, as it contains all the information that you need to fill out the mandatory fields in the rules policy.

In this example, you have all the information you need to create an EPM rule for `HPUpdate.exe`:

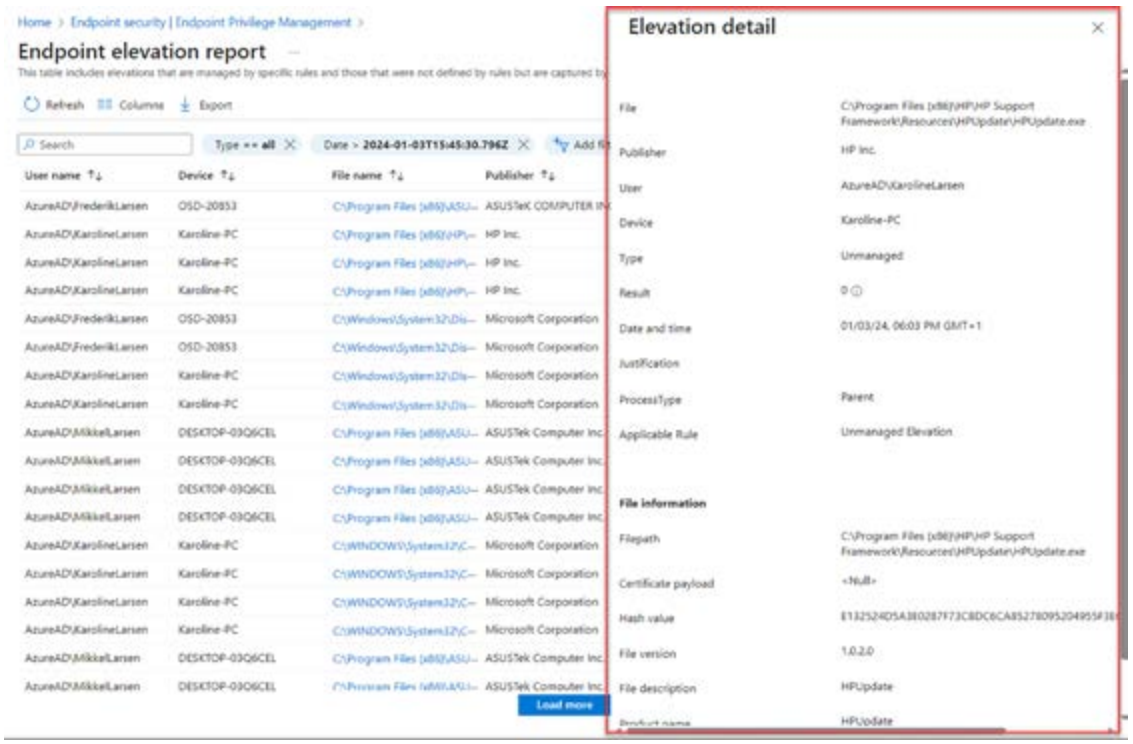


Figure 11.37: EPM elevation report

Managed elevation report

Here, you can see the status of elevations that occurred inside the elevation with a management policy, so it will not show unmanaged elevations.

Elevation report by applications

With this report, you can see all elevations, both managed and unmanaged by application. You will get a report with a list of applications and an elevation count per app, and you will also get a minimum of information on the app.

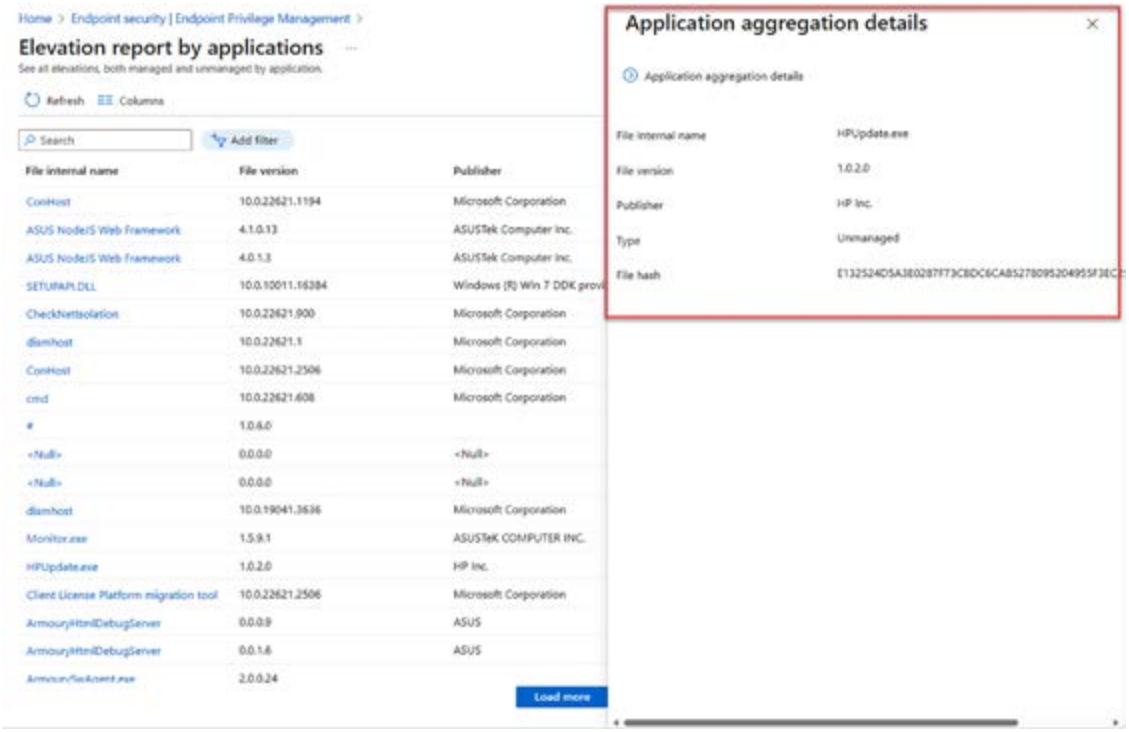


Figure 11.38: EPM elevation report by applications

Elevation report by Publisher

Here, you can see the number of elevations by each publisher and will get the elevation count per publisher. The report does not provide you with any details for each elevation.

Elevation report by User

This lets you see the number of elevations by each user, where you get the elevation count per user. The report does not provide you with any details for each elevation

This concludes the section on EPM reporting. Next, we will share where the EPM Agent is installed on your end users' devices.

EPM Agent

A common question we get asked about EPM is where the binaries are located on the end users' Windows devices. In the figure below, you can see that location:

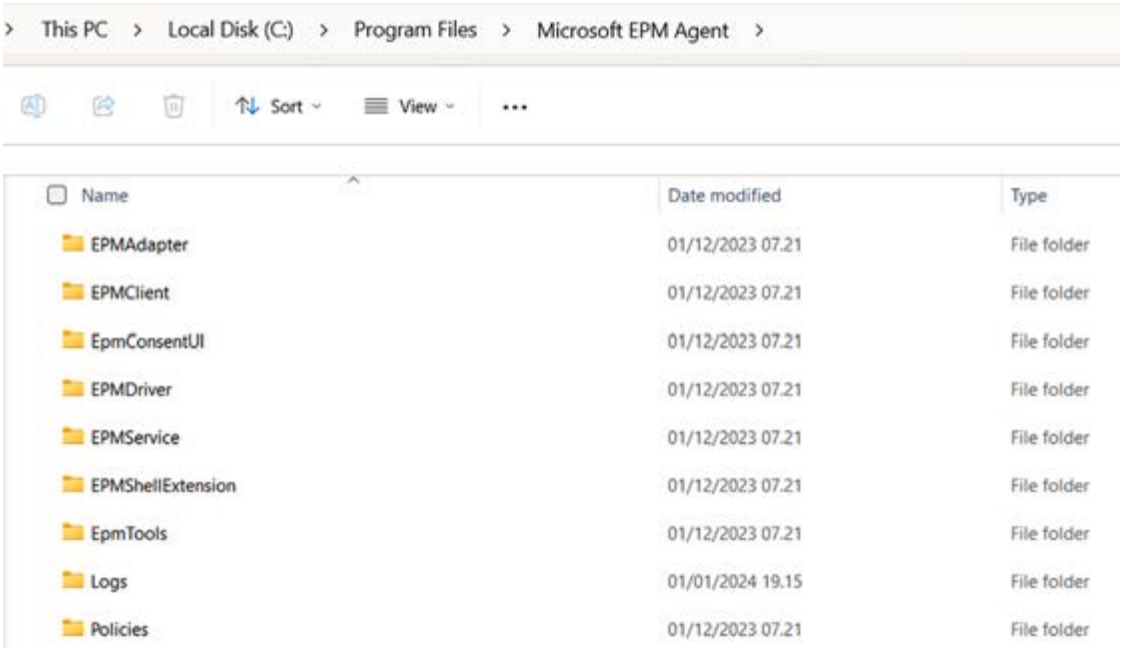


Figure 11.39: EPM Agent files

How do you get your users' account type to Standard?

For new cloud-provisioned devices, you should set **User account type** to **Standard**, as that is more secure and recommended by Microsoft. When the user onboards that device using Windows Autopilot, they'll become a standard user on that device. You can read more about Windows Autopilot in *Chapter 7*, *Windows Autopilot*.

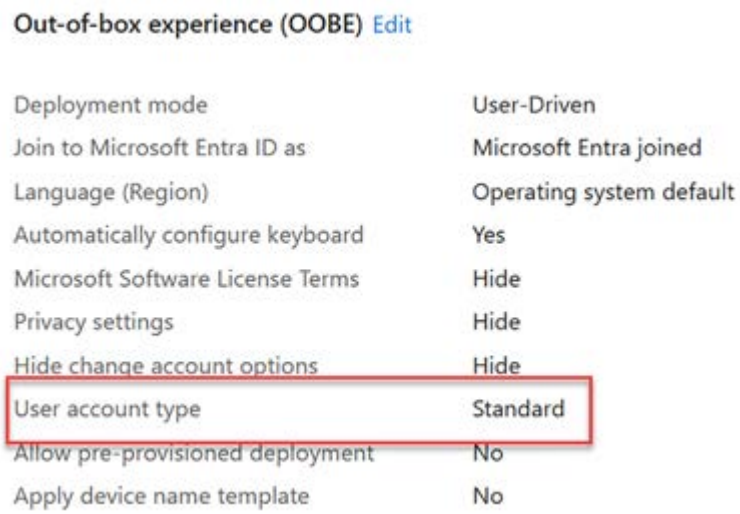


Figure 11.40: Autopilot Profile Standard user

For devices that are already up and running in your environment, you can configure a Microsoft Intune policy that ensures that your user is not a member of the local administrator group.

Configure policy for standard user

If your end users already are local admins on existing devices and you need to change that to standard users, the easy way is to create a policy in Intune that configures who is a member of your local administrator group.

To configure the elevation setting policy, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Endpoint Security** | **Account Protection** | **Create Policy**:

    - **Platform**: Select **Windows 10 and later**
    - **Profile**: Select Local user group membership

    Local user group membership policies help to add, remove, or replace members of local groups on Windows devices.

2. Enter a name for the policy and click **Next**.

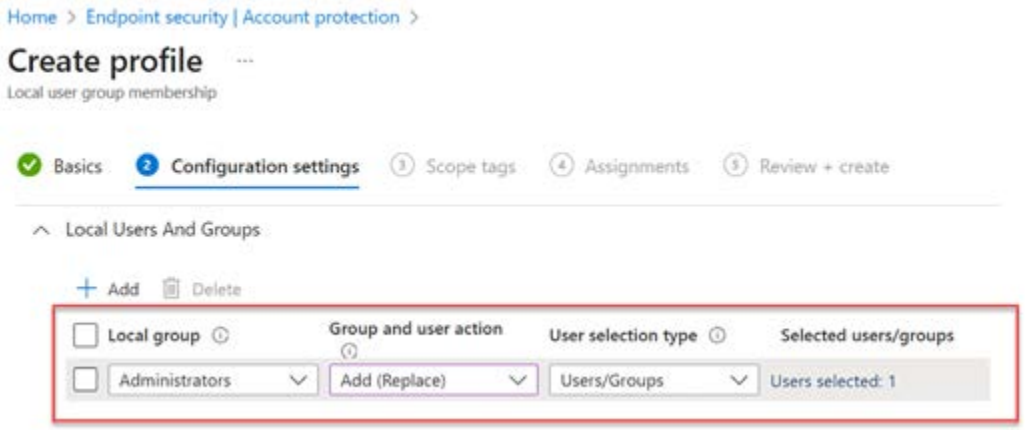


Figure 11.41: Local user group membership

Leave **Local group** as **Administrators**, and change **Group and user action** to **Add (Replace)**. Then, select a new user/group to be a member of your local administrator group.

Group and user action has three options:

- **Add** (Update): Adds members to a specified group while keeping the current group membership intact.
- **Remove** (Update): Removes members of a specified group while keeping the current group membership intact.
- **Add** (Replace): Replaces the current membership of a specified group with a newly specified group.

If you just want to leave the two default Entra ID **Security Identifiers** (**SIDs**) (Global admin and Cloud Desktop administrator) in the local admin group, you can look up the group SID in the local admin group on devices that are already joined to Entra.

You need to put the users or groups you want to add to the local administrator group in the **Add users** list in the following screenshot.

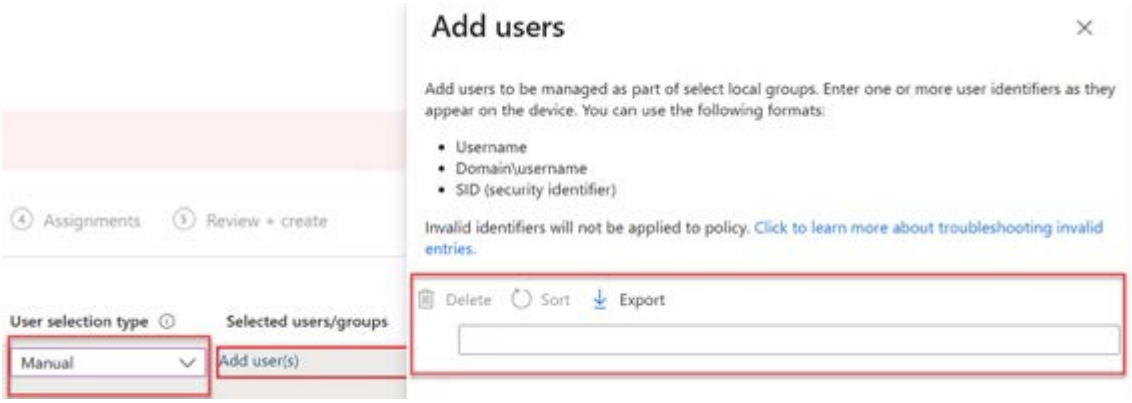


Figure 11.42: Add users



Note

You do not need to care about local naming for the administrator group as the policy in the background is using the SID and not the name of the group, which is different from language to language.

This concludes the section on how to manage your local Windows administrator groups. In the next section, we will cover the end user workflow in EPM.

End user process

Here, we will show the end user workflow when the user starts a line of business app installation:

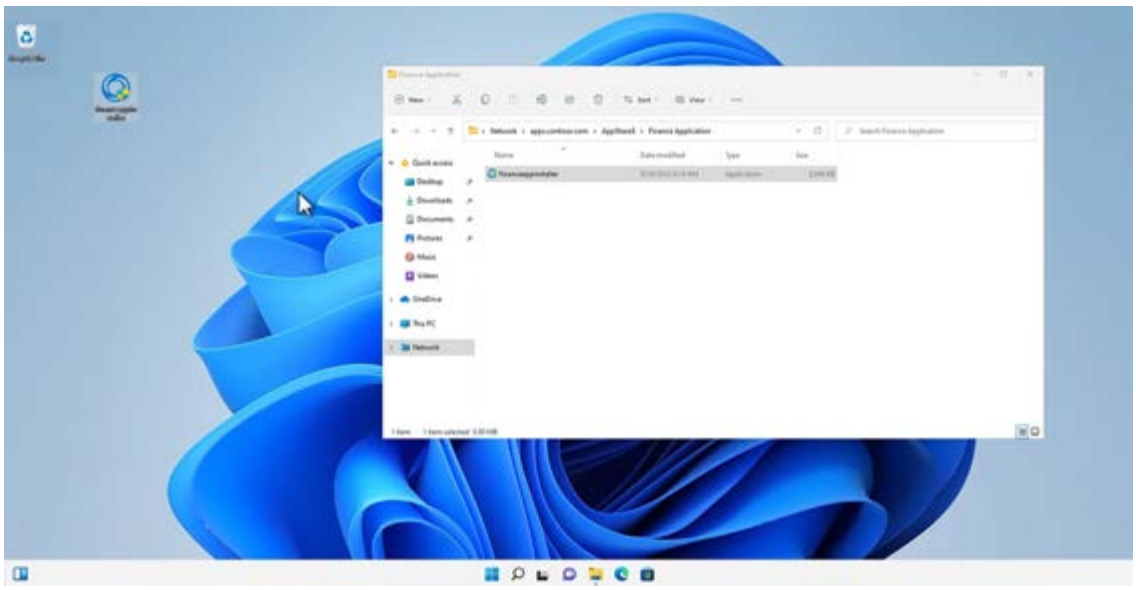


Figure 11.43: Windows installation file

1. EPM starts and will ask for business justification.



Figure 11.44: EPM business justification



NOTE

If you have configured support approval in your **elevation settings policy**, the request will be sent to the Intune backend service – otherwise, if you just have the required business justification or Windows authentication, the application will have been launched with elevated privileges.

The Support Approved workflow is in private preview at the time of writing.

2. The request was sent – we are now waiting for approval.

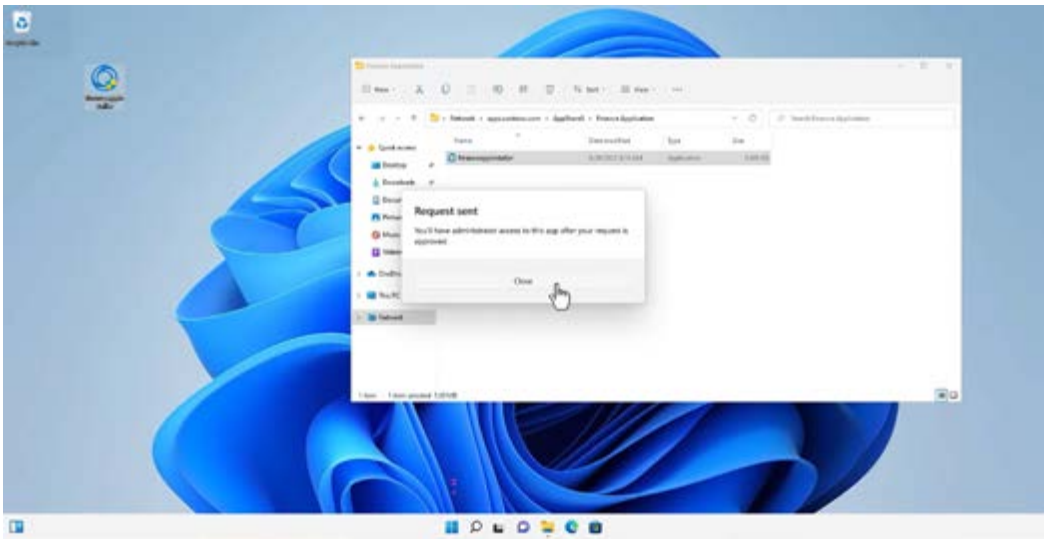


Figure 11.45: EPM approval request sent

3. The IT admin receives an elevation request for approval inside the Intune admin center.

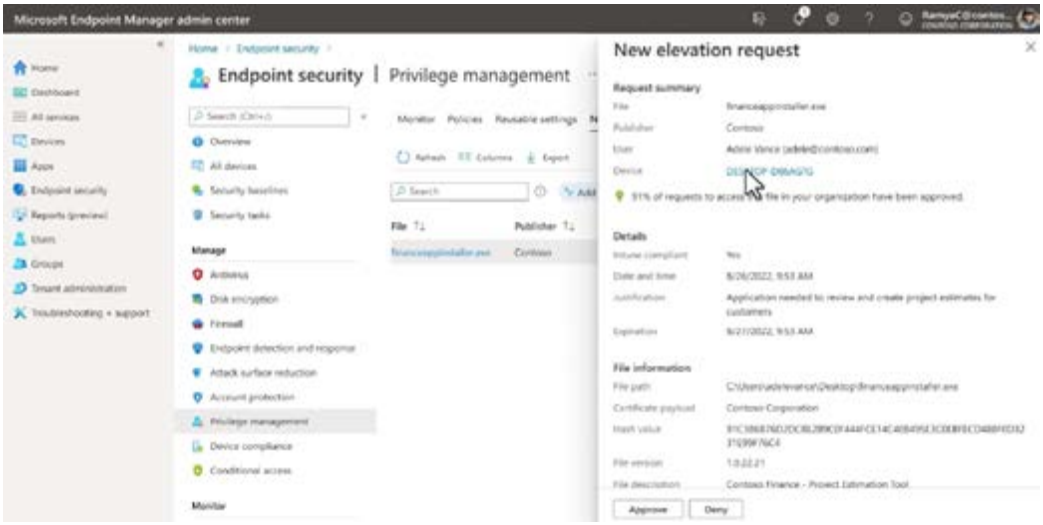


Figure 11.46: New elevation request as seen in the Intune admin center

4. After the IT administrator gets the notification and approves the request, the user can retry installing or opening the application.

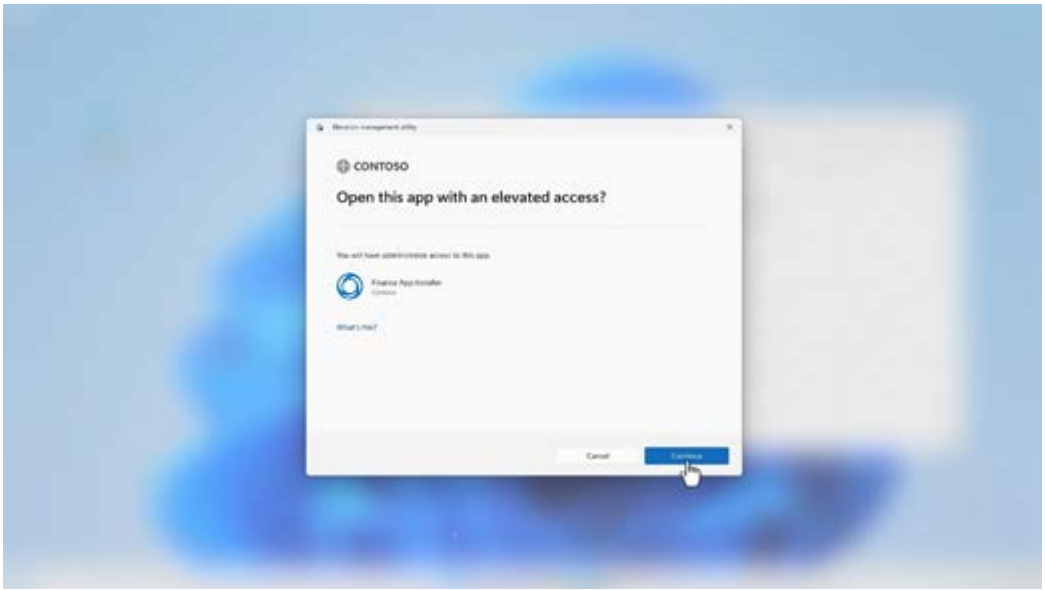


Figure 11.47: EPM – user gets access

5. The installation can now run successfully.

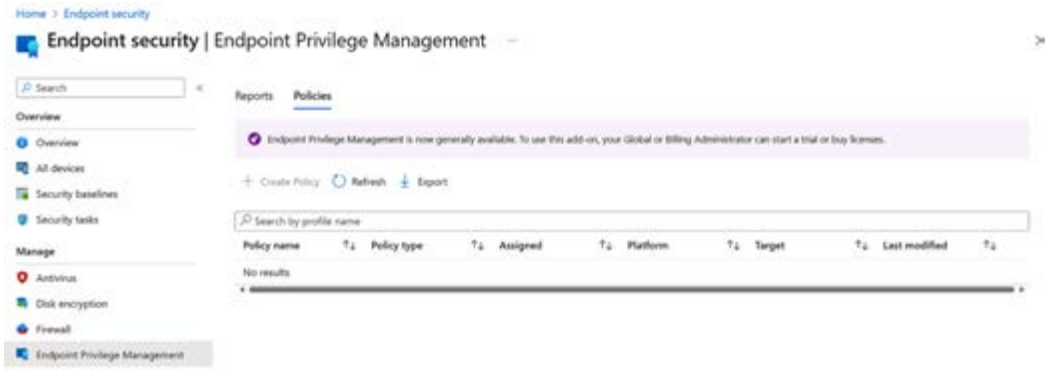


Figure 11.48: EPM without a license

If you do not have an active EPM license in your tenant, then the **Create Policy** option will be grayed out. We often get asked how EPM handles local admin accounts and passwords. That is not what EPM is built for – we highly recommend you take a look at the Windows Local Administrator Password Solution we cover in *Chapter 13*, *Identity and Security Management*, of this book.

Another question we get asked is how EPM blocks an unwanted app from running on a device. That is not what EPM is built for either, but there are a lot of built-in features in Windows that can help with this:

- Application Control for Business (we cover this in *Chapter 13*, *Identity and Security Management*)
- SmartScreen
- **Attack Surface Reduction** (**ASR**)
- Microsoft Defender – **Potentially unwanted applications** (**PUA**)

In *Chapter 13*, *Identity and Security Management*, we talk about how to implement Application Control for Business. Here are two great places to find the recommended block for files and drivers that you can implement in your environment:

- Applications that can bypass WDAC and how to block them: `https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/applications-that-can-bypass-wdac`
- Microsoft recommended driver block rules: `https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/microsoft-recommended-driver-block-rules`

This concludes the section on EPM. Now, we will continue with Enterprise App Management.

Enterprise App Management

The initial release of the Enterprise App Management solution offers a new Enterprise App catalog. This catalog is hosted by Microsoft and, at launch, contains over 100 first- and third-party apps.

See the full list of available applications here: `https://learn.microsoft.com/en-us/mem/intune/apps/apps-enterprise-app-management#apps-available-in-the-enterprise-app-catalog`.

The key capabilities of Enterprise App Management are:

- Securely hosted enterprise app catalog for first- and third-party applications.
- Guided updating processes to save time and resource hours.
- With access to the Microsoft Graph APIs, you can develop your own customized scripts to automate apps.

The solution helps IT save time by streamlining the process of discovering and packaging apps:

- **Streamlined application management**: Reduces the complexity of managing Microsoft and third-party apps across your organization by streamlining the process of discovering, packaging, and updating apps directly from the Microsoft Intune console.
- **Reduced security risks and vulnerabilities**: Deploys app fixes quickly to mitigate risk immediately with proactive discovery of security vulnerabilities.
- **Stay current with updates and alerts**: Keeps apps up to date and secure by proactively identifying and updating them using update notifications and guided updating.

Now, we're going to explain how it works.

Installing applications via Enterprise App Management

In order to install applications via Enterprise App Management, follow these steps:

1. First, go to **Apps | Windows** in the Microsoft Intune admin center.

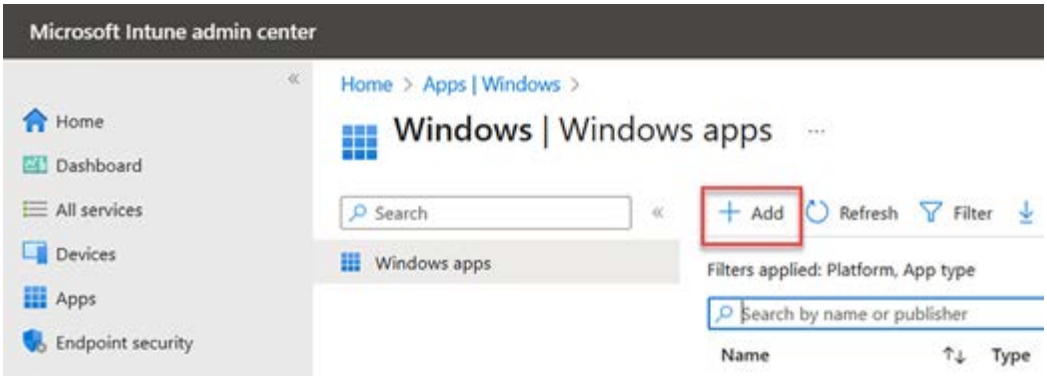


Figure 11.49: Windows apps

2. Click **Add**.

3. Select **Enterprise App Catalog app** for **App type.**

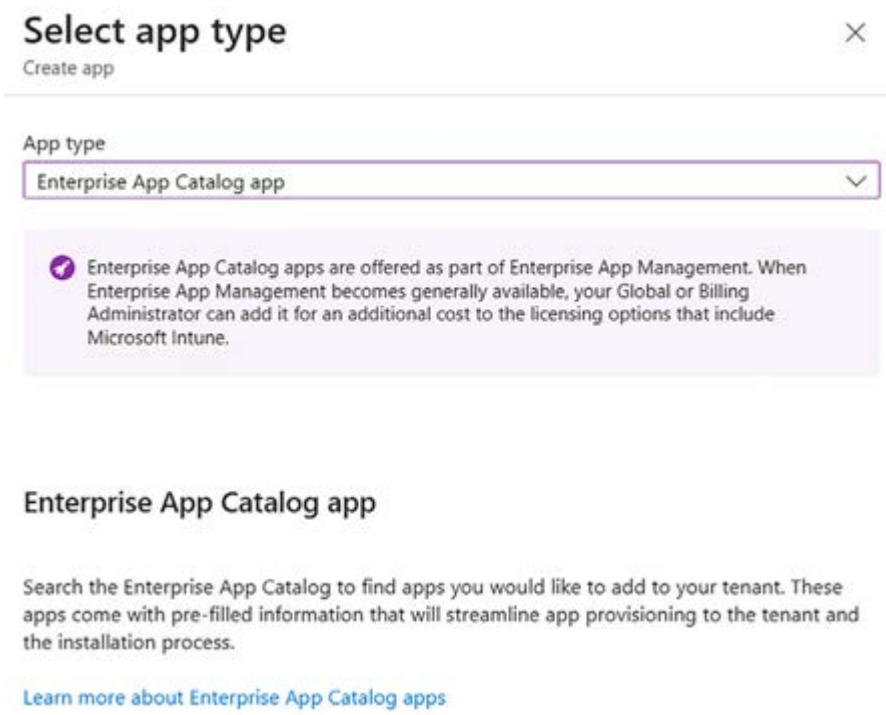


Figure 11.50: Enterprise App catalog app

4. Click **Search the Enterprise App Catalog.**

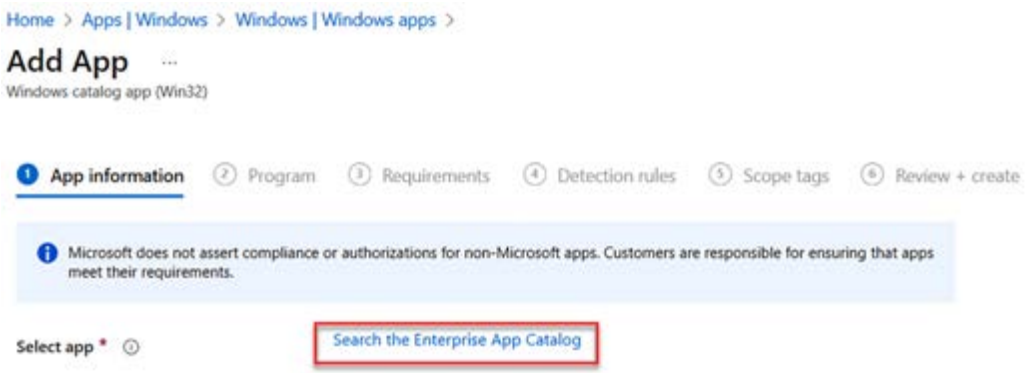


Figure 11.51: Search the Enterprise App Catalog

5. For application installations, click **Select app** and search for the application you want to install from the **Enterprise App catalog.**

In this example, we will add **Adobe Reader XI** to our Intune tenant from the **Enterprise App catalog**, so that we can deploy it to our end users' devices.

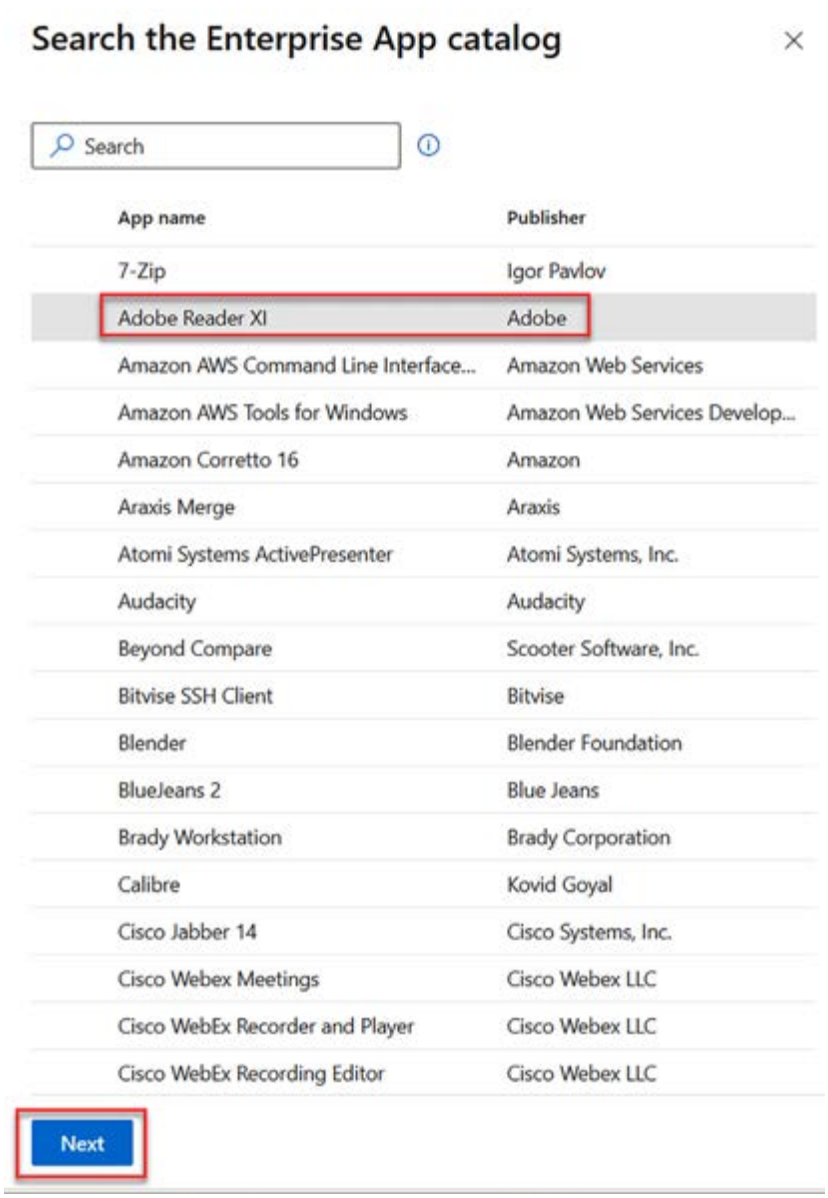


Figure 11.52: Adobe Reader XI

6. Select **Reader XI** as the Adobe package, based on your language preference.

This is one of the great benefits of using Enterprise App Management, as it allows easy version management of apps.

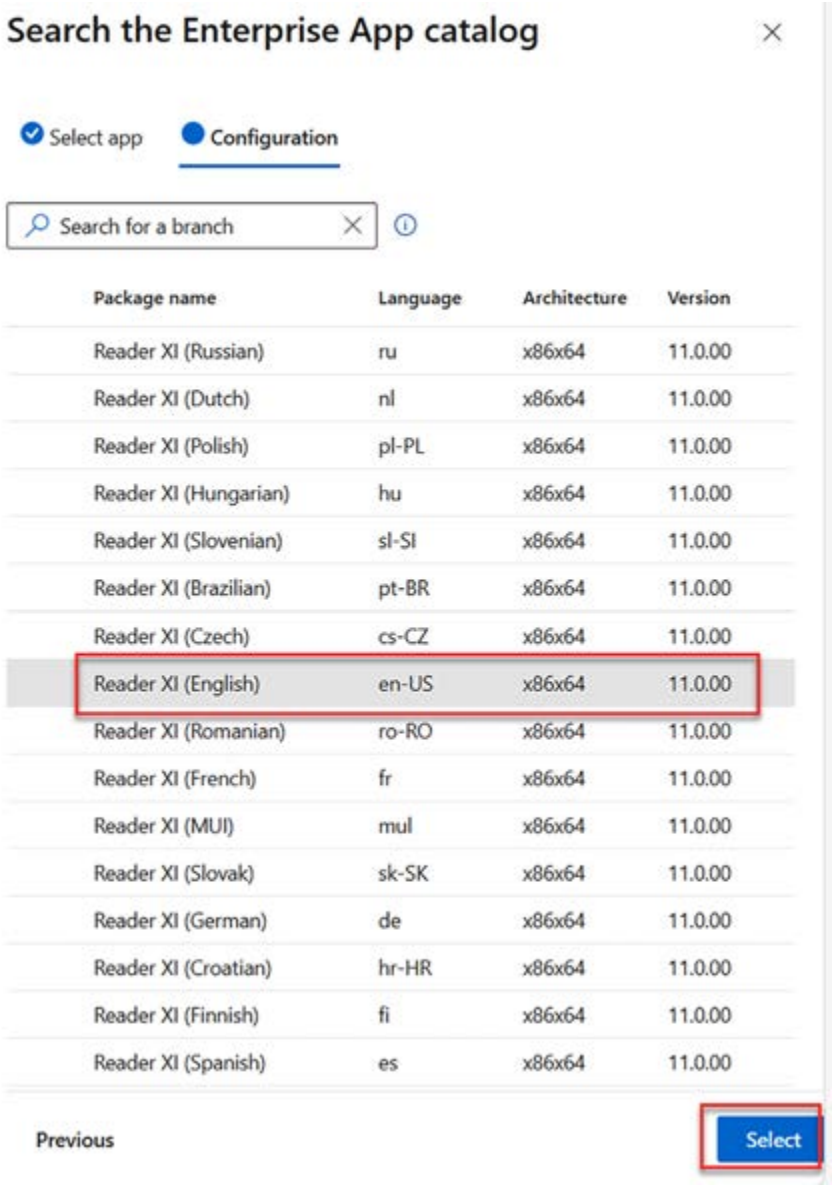


Figure 11.53: Select the right language and version

7. Customize the application as you normally would do via Intune when creating a Win32 app – you have all the same options here as the Win32 app model gives you.
8. The benefit is that everything is prefilled for you as an IT administrator.

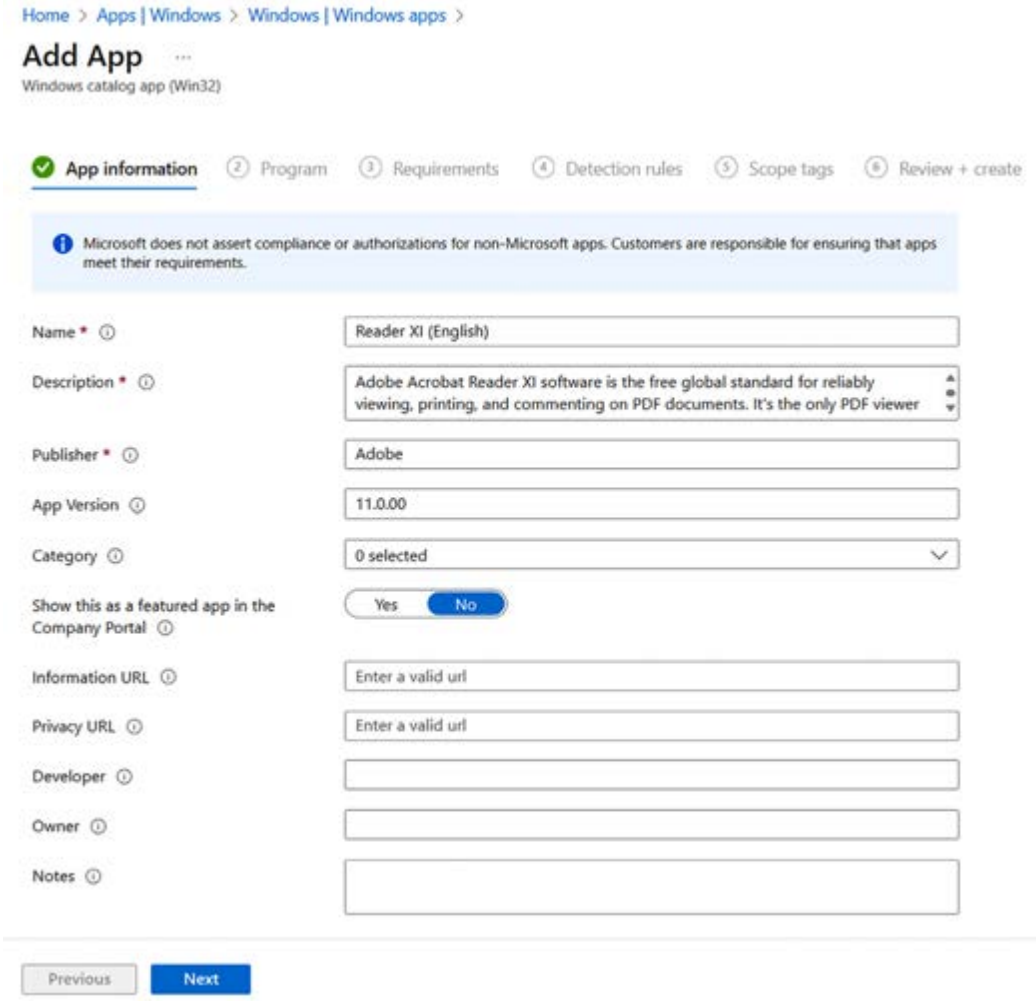


Figure 11.54: Application information

9. Customize the install and/or uninstall commands (if needed). The command-line parameter in the apps from Enterprise App Management has all the correct parameters to silently install/uninstall the application on your end users' devices.

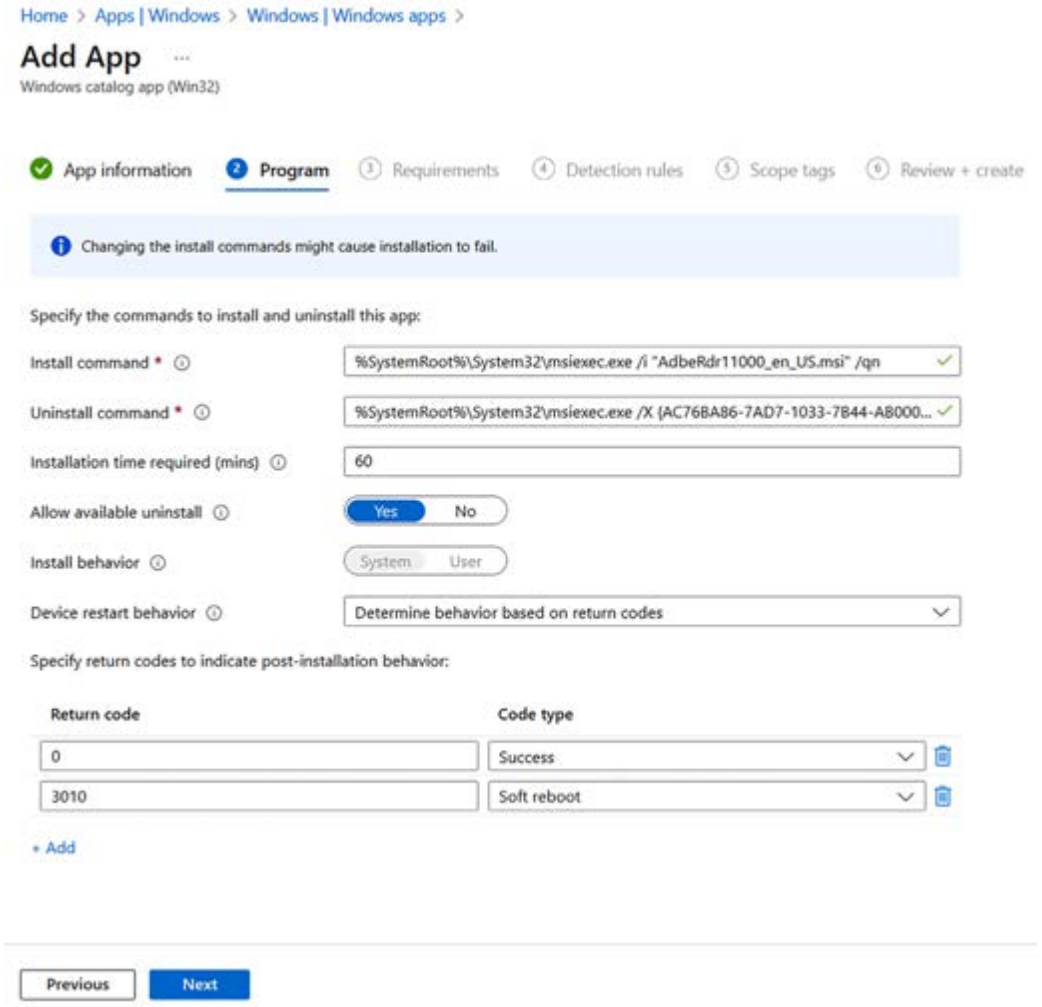


Figure 11.55: Program

10. Configure additional requirements, if needed, or click **Next**.

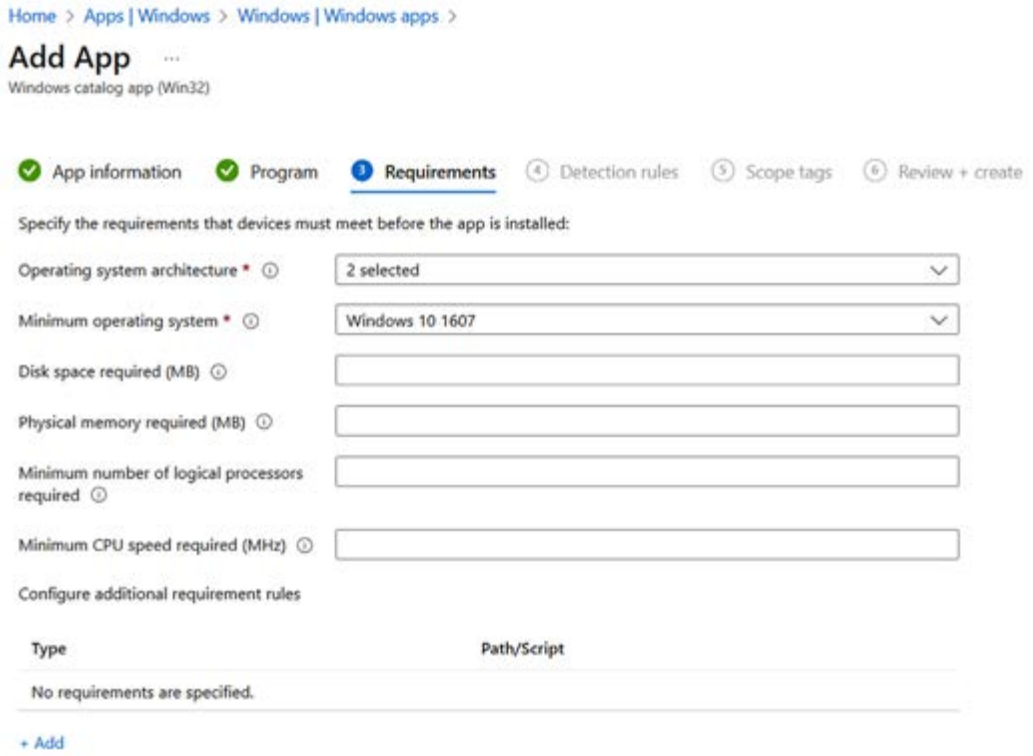


Figure 11.56: Requirements

11. Define detection rules to ensure that Intune knows when the application is successfully installed.

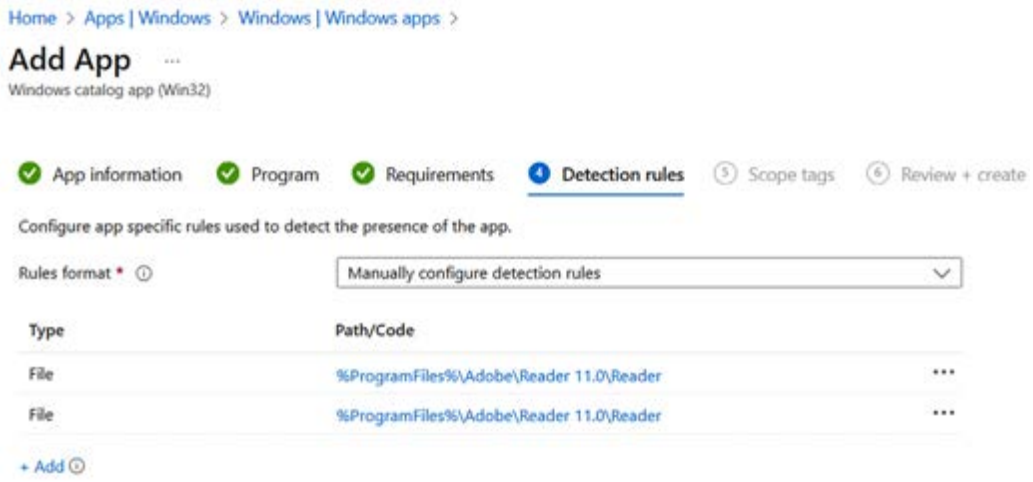


Figure 11.57: Detection rules

12. Click **Next** to continue to the **Scope tags** blade, where you should also click **Next** (to select the scope tags).

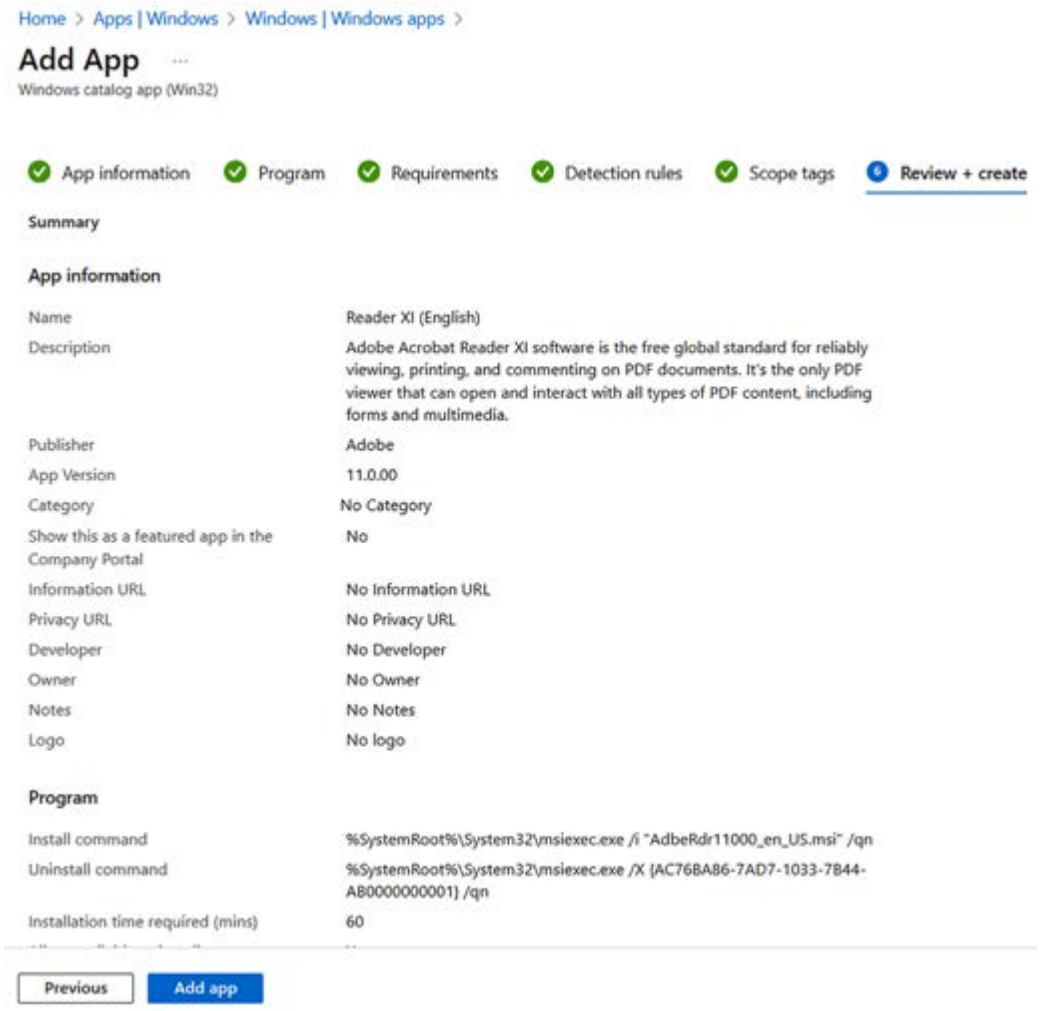


Figure 11.58: Review + create

13. On the **Review + create** blade, click **Add app**.

Enterprise App Management will now start downloading the app in the background and put it in your tenant as any other Win32 app, and when that is done, you are ready to deploy the app to your Windows endpoints.

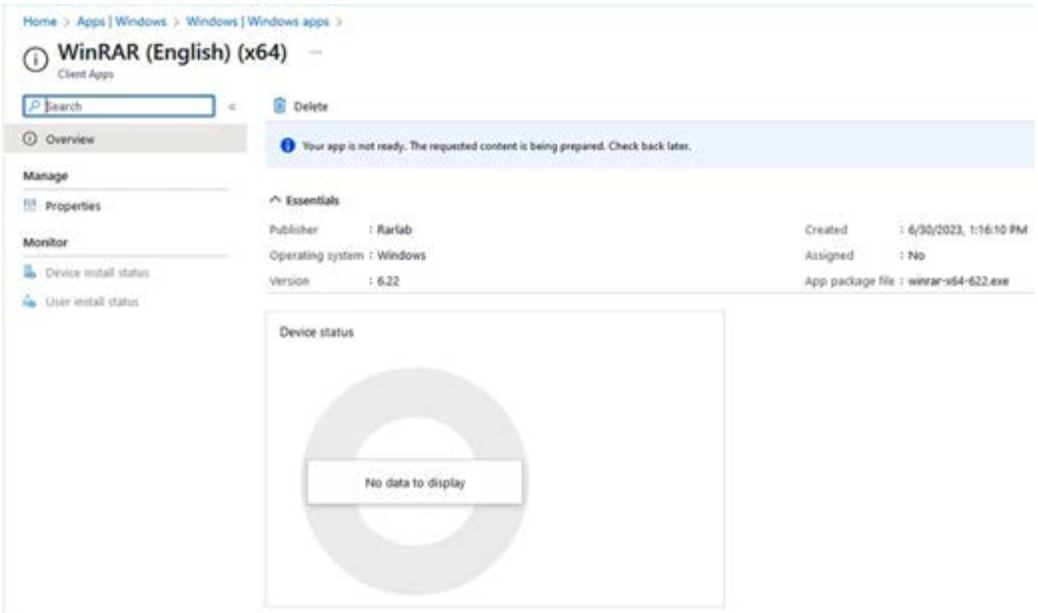


Figure 11.59: Your app is not ready yet

While your new app is being downloaded and created in your Intune tenant, the app will show this information text: **Your app is not ready. The requested content is being prepared. Check back later**.

Let's now move to application management in terms of updates!

What about enhanced application updates?

With Enterprise App Management, Microsoft also introduced the capability to provide updates for Windows (Win32) catalog apps in the future. As this is not in production at the time of writing this book, some of the screenshots and/or functionality may change. This works very simply and is straightforward. We will explain how it works for this example app:

1. Go to **Apps | Updates for Windows (Win32) catalog apps.**

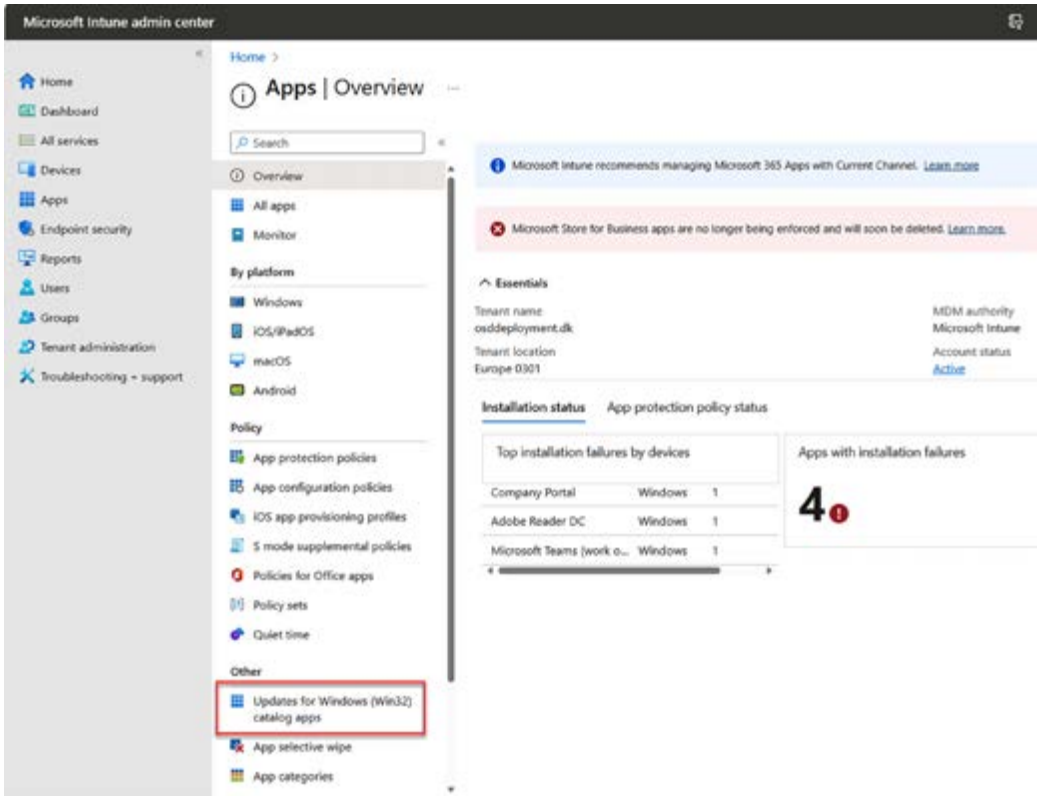


Figure 11.60: Updates for Windows (Win32) catalog apps

2. Click on the three dots (**...**) to the right of the application you want to update.

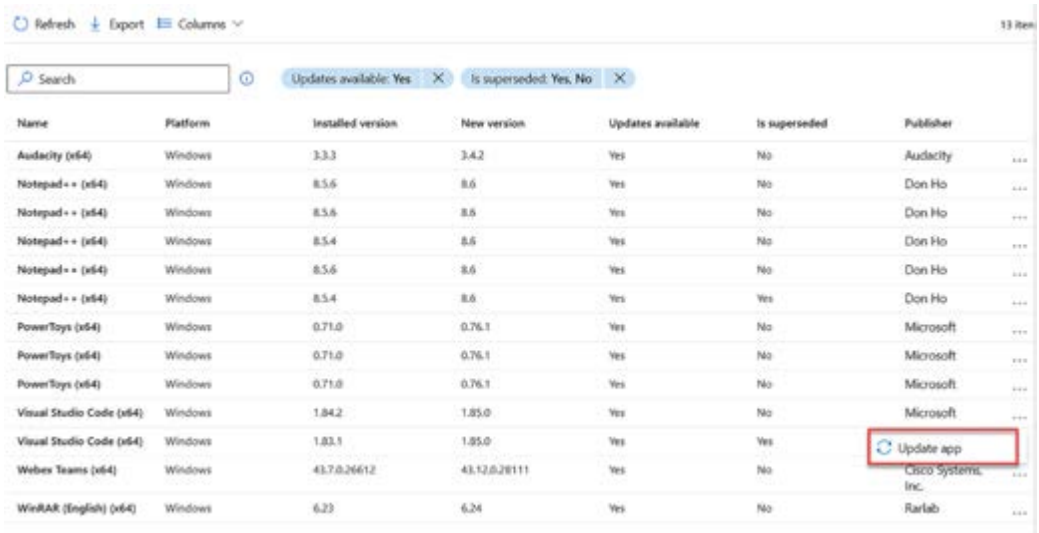


Figure 11.61: Update app

3. Change the app version or name (if needed). We will cover the most important steps here, and those are under the **Supersedence** blade.
4. In this case, we provided `Visual Studio Code` (x64) as the name.

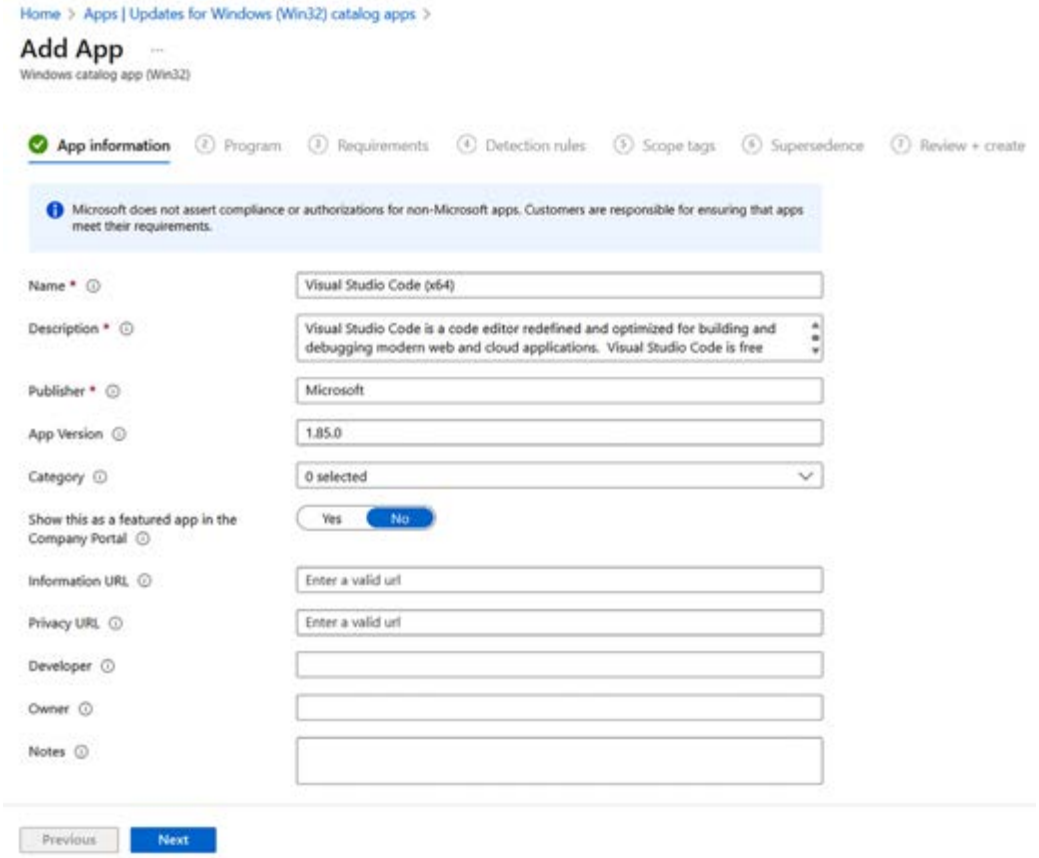


Figure 11.62: App information

You need to go through the wizard the same way as when you created an app for the first time. You can change settings if you need to – otherwise, just stop at the **Supersedence** tab.

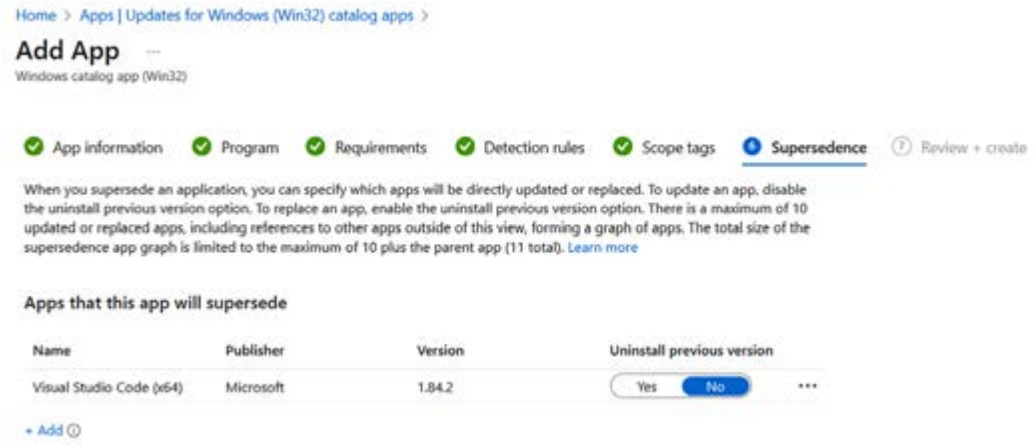


Figure 11.63: Supersedence

5. Toggle the **Uninstall previous version** option for the app.
6. Provide the app versions that you want to replace by clicking on **+ Add** to add the newer version of the app.

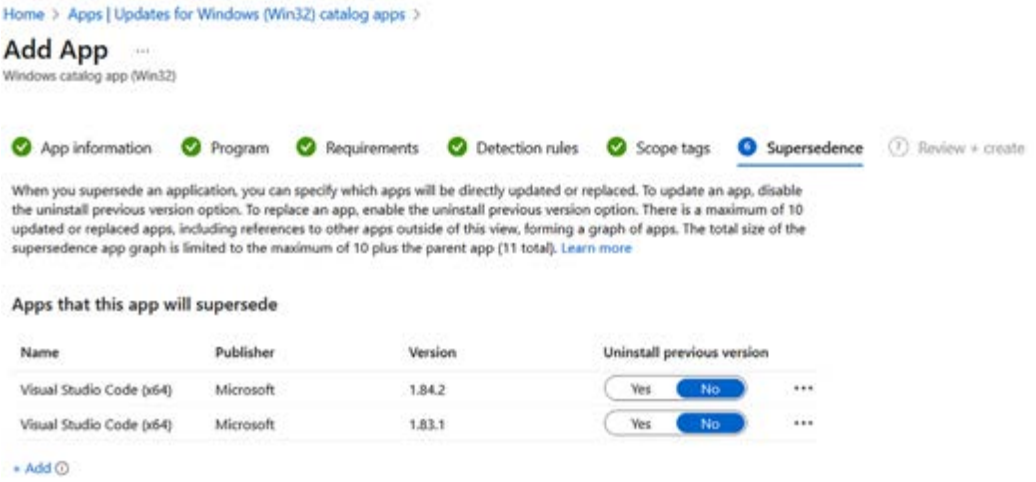


Figure 11.64: Supersedence of multiple apps

7. Once ready, check the summary once more, and the application will auto-update to all your Windows endpoints based on the configurations set per Enterprise App Management!

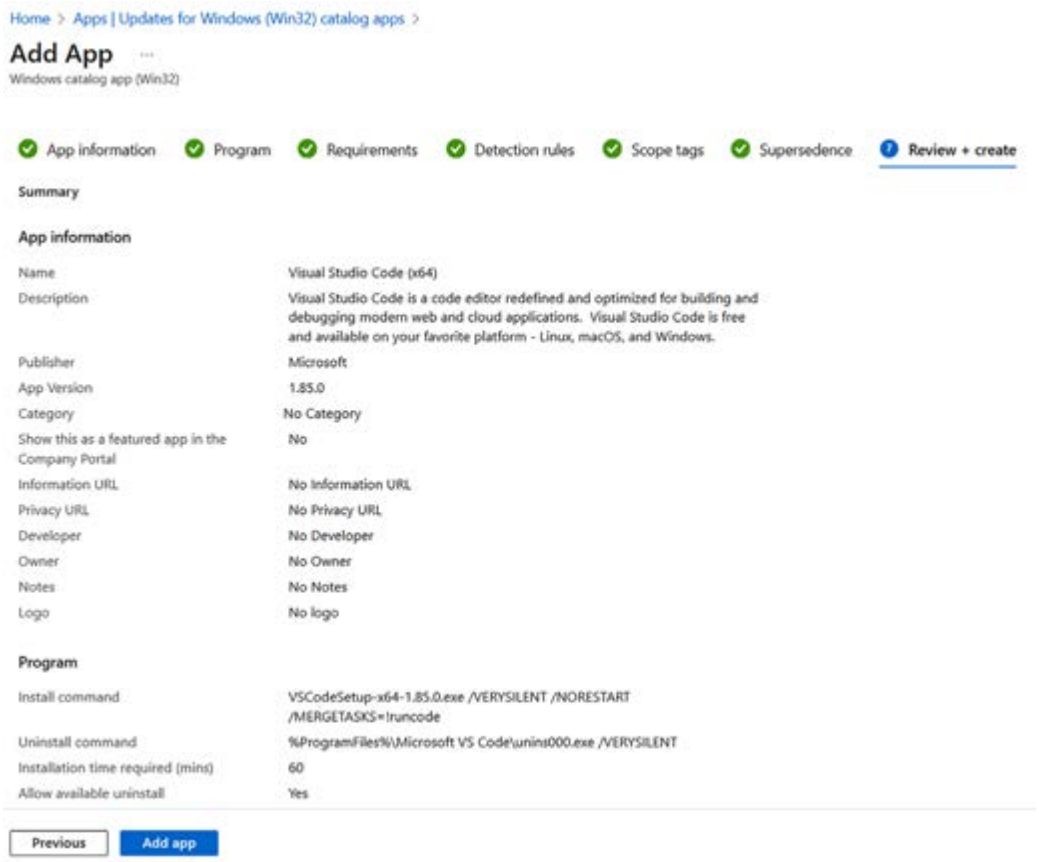


Figure 11.65: Review + create

In the Windows apps overview blade, you can filter by app type – **Windows catalog app** (**Win32**) – and then you will be able to see all apps that have been created or added by you using Enterprise App Management.

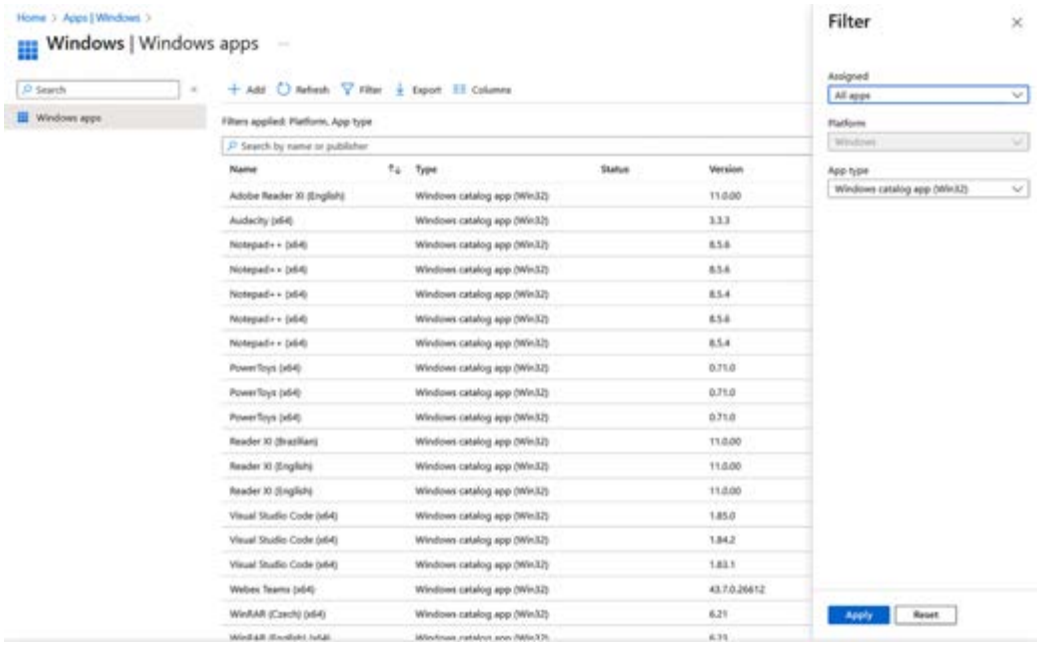


Figure 11.66: Filter apps by Windows catalog app

Cloud certificate management (Cloud PKI)

Cloud PKI offers several advantages over traditional on-premises PKI. Cloud PKI provides the following benefits:

- **Lower total cost of ownership (TCO)**: Cloud PKI eliminates the need for expensive hardware and software, reducing the overall cost of ownership. Reduces on-premises CA workload and operations (patching and maintaining servers, etc.).
- **Increased security**: Cloud PKI providers have the expertise and resources to ensure the security of the infrastructure, which is often more secure than on-premises solutions.
- **Easier certificate management**: Cloud PKI solutions offer a centralized platform for certificate management, making it easier to manage certificates across multiple domains.
- **Less complex**: With a cloud-based infrastructure, you do not need to implement and secure a **Simple Certificate Enrolment Protocol** (**SCEP**) server as is it built into the solution. No need for a reverse proxy (Entra application proxy or third-party).

Authentication with certificates is a secure and seamless experience for the user. By establishing user or device identity as trustworthy, devices and users can request a signed certificate, enabling the user to present it to other services for authentication purposes.

With Microsoft Intune Cloud PKI, you can manage your cloud certificates in the same place as you manage your endpoints.

A migration from on-premises to cloud-managed certification can not only streamline processes and reduce management costs but it also drastically simplifies the delivery and management of certificates and enhances security without dedicated **Subject Matter Experts** (**SMEs**) to manage.

How does the process work?

When a company needs to create a new PKI or update an existing one, the IT administrator needs to create a root CA and an issuing CA, and install an SCEP server – that part of the process is made easy with Cloud PKI. This process is shown in the figure below.

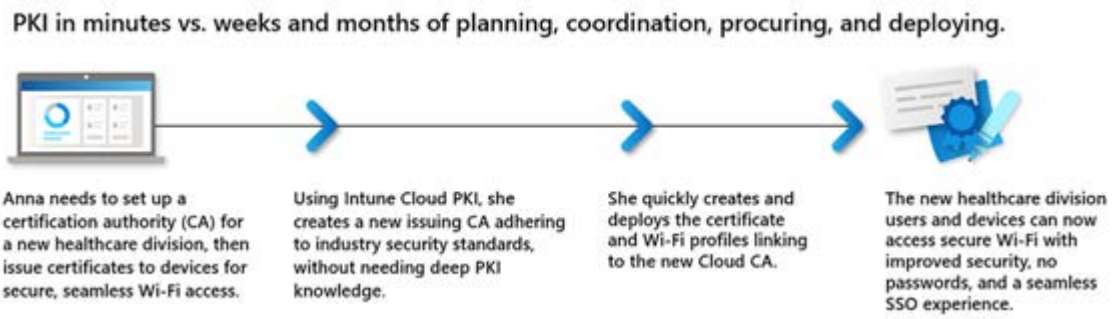


Figure 11.67: PKI process

A two-tier PKI hierarchy is a design that meets most companies' needs. It is a compromise between one- and three-tier hierarchies. In this design, there is a root CA and a subordinate issuing CA. The level of security is increased because the root CA and issuing CA roles are separated.

Two-tier PKI hierarchy

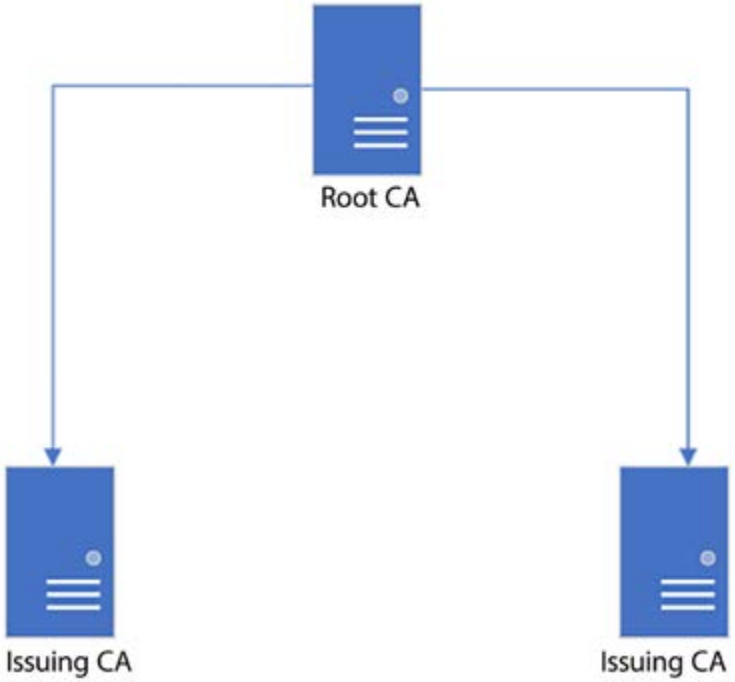


Figure 11.68: Two-tier PKI hierarchy

The chain of trust is a critical concept in the realm of SSL certificates. It ensures that your certificate can be trusted by browsers and other clients. Here's how it works:

- **Root certificate**:
  - At the heart of the chain lies the root certificate. This digital certificate belongs to the **Certificate Authority** (**CA**) that issued it.
  - Root certificates are pre-installed in most browsers and are stored in a "trust store."
  - These certificates are closely guarded by the CAs themselves.
- **Intermediate certificates**:
  - Think of intermediate certificates as branches of the root certificates. They act as middlemen between the protected root certificates and the server certificates issued to the public.
  - There's always at least one intermediate certificate in a chain, but there can be more.
  - These intermediates help establish the link between the root and the server certificate.

- **End entity certificates:**
  - **Users:** Individuals using PKI certificates for secure communication (e.g., email encryption, digital signing, etc.)
  - **Devices:** Servers, machines, cryptographic hardware, and other systems (e.g., SSL/TLS certificates for websites)

The certificate chain works as described in *Figure 11.69*.

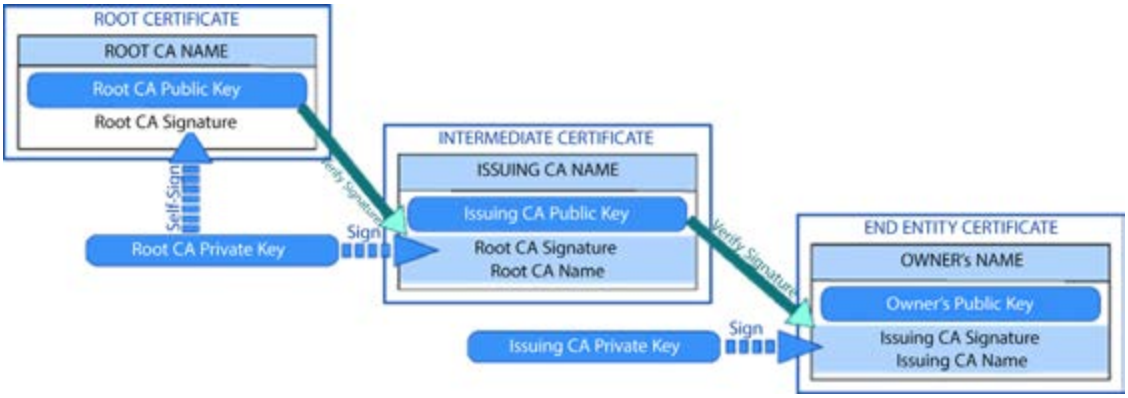


Figure 11.69: Certificate trust chain

The following are the basic steps for creating a policy configuration from the Microsoft Intune admin center:

1. First of all, we need to create the root CA in our Cloud PKI infrastructure.

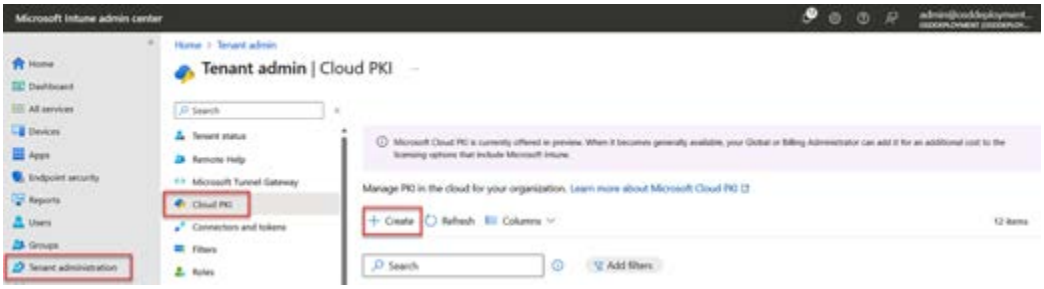


Figure 11.70: Create Cloud PKI

2. In the **Basics** section, you need to give the root CA a name.

3. First, you need to select **Root CA** or **Issuing CA** as the CA type. You need a root CA before you can create an issuing CA.

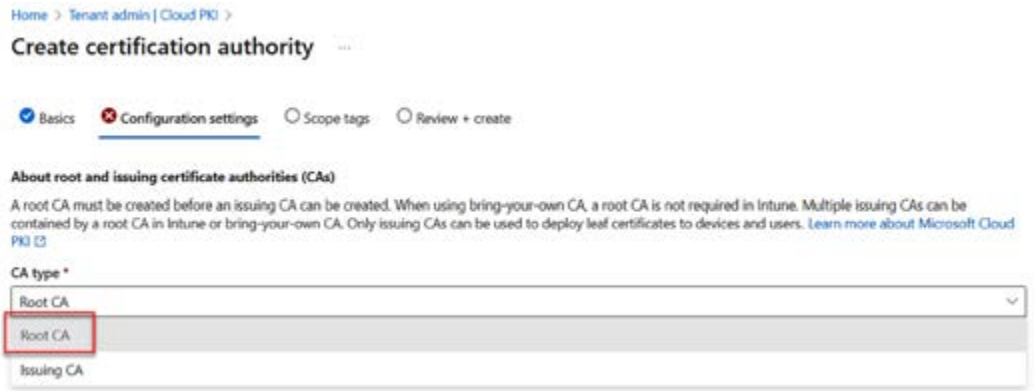


Figure 11.71: Root CA

4. You also need to select a **validity period** that matches your organization's policies. In the example, we will make the validity period 20 years.

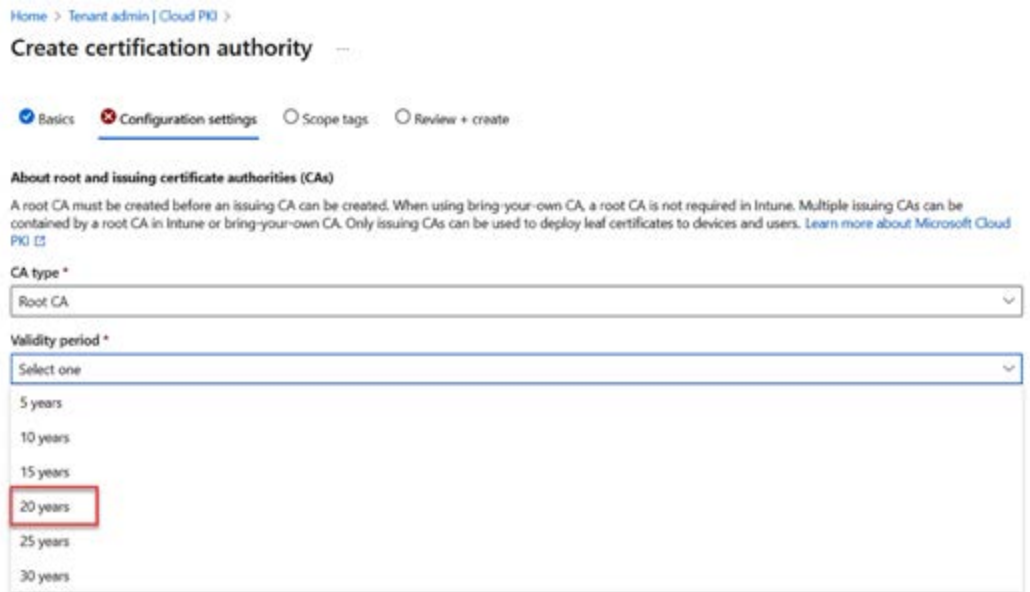


Figure 11.72: Validity periods



NOTE

For enhanced validity periods, please be advised that selecting a greater number of years for the root CA's validity is advisable (if required). This is because the validity period for the issuing CA cannot exceed the duration specified in the root CA's certificate. Therefore, to ensure longer validity for downstream certificates issued by the issuing CA, it is recommended to set a longer validity period for the root CA itself.

This practice enables you to maintain consistent and extended validity across your certificate hierarchy, offering enhanced security and operational efficiency.

5. You need to select **Extended Key Usages:** in this example, we are selecting **Client auth, Smartcard logon, Server auth**, and **Code signing**.



Figure 11.73: Extended Key Usages

6. Next, fill out the subject attributes that you want to leverage in your organization.
7. **Common name (CN)** is the only mandatory attribute.



Figure 11.74: Root CA Subject attributes

8. You need to select the key size and algorithm for your root CA – when you create an issuing CA, it will get the same values.



Figure 11.75: Key size and algorithm

9. Assign **scope tags** if you need to, and then click **Next.**
10. Now you just need to review and create the settings you have selected before your new root CA will be deployed in your tenant.



NOTE

Once you have created the root CA, you cannot change the values. The only option is to create a new one if you require different values.

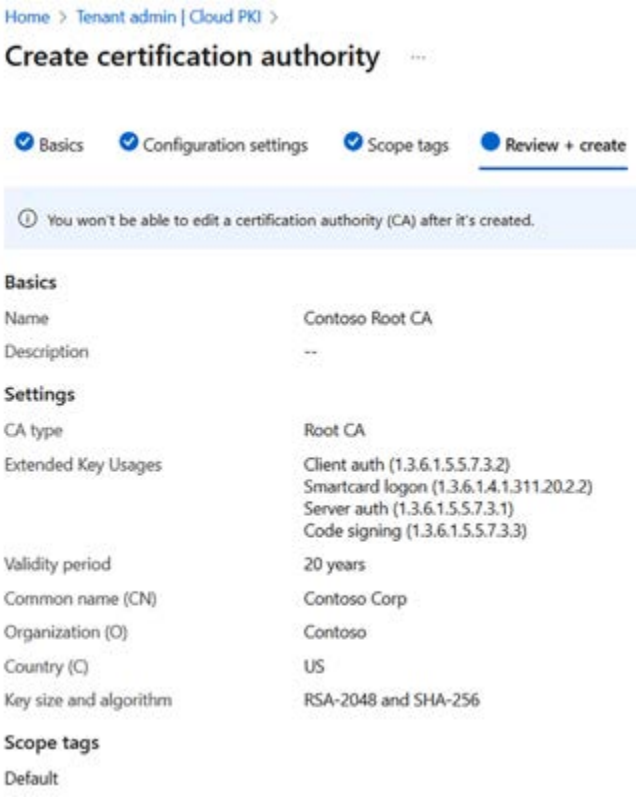


Figure 11.76: Review + create

When the root CA is deployed, you can start creating the issuing CA in the same way as you started the root CA wizard:

11. You need to give the issuing CA a name as well.

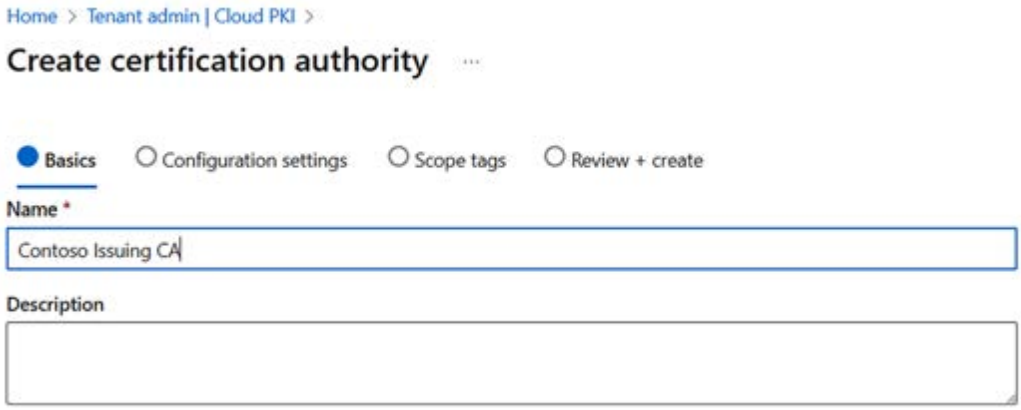


Figure 11.77: Cloud PKI Issuing CA, Basics

12. In the CA type field, select **Issuing CA**, then from the drop-down box for **Root CA source**, select either **Intune** or **Bring your own root CA**.

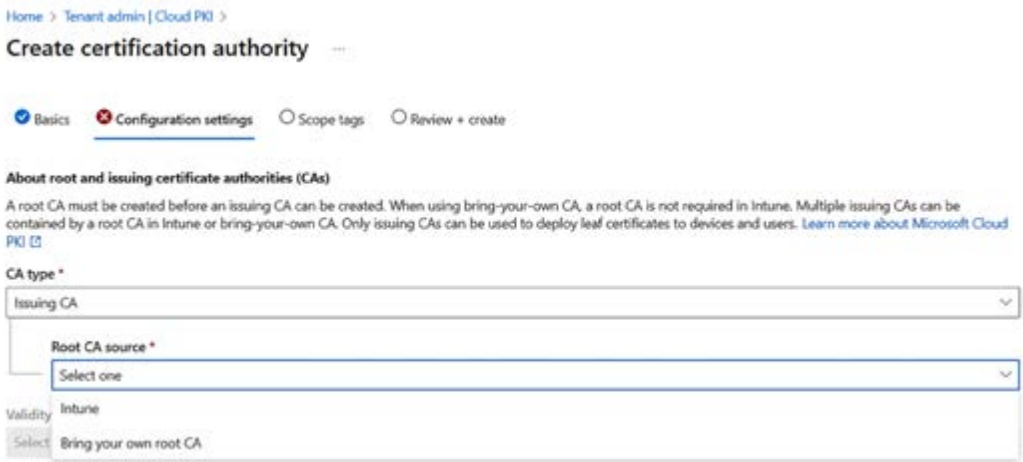


Figure 11.78: Cloud PKI Issuing CA, Configuration settings

13. If you already have an on-premises PKI infrastructure where you want to leverage Cloud PKI instead of your on-premises issuing CA and SCEP server, this is the option you will choose. Then you use the properties in the wizard to create a **Certificate Signing Request** (**CSR**). The CSR must be signed by your private CA before this CA can be enabled.
14. In this case, we will create a new completely cloud-native PKI infrastructure leveraging the **Root CA** that we just created – so we will select **Intune**.

15. Then, you can select the **Root CA** that you just created; in this case, search for **Contoso Root CA.**

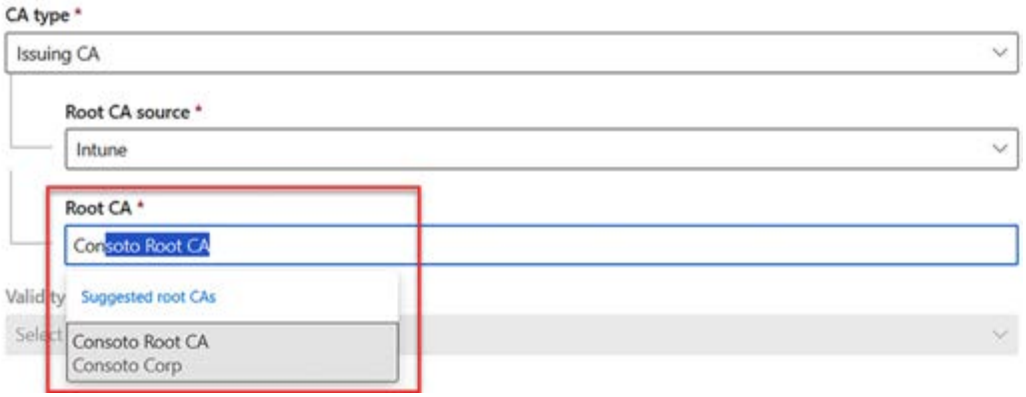


Figure 11.79: Root CA source and Root CA

16. Then, you need to select the validity period. In this example, we are setting the validity period for **2 years.** Here, as you can see, you are only able to select a validity period that is longer than the validity period set in the root CA.

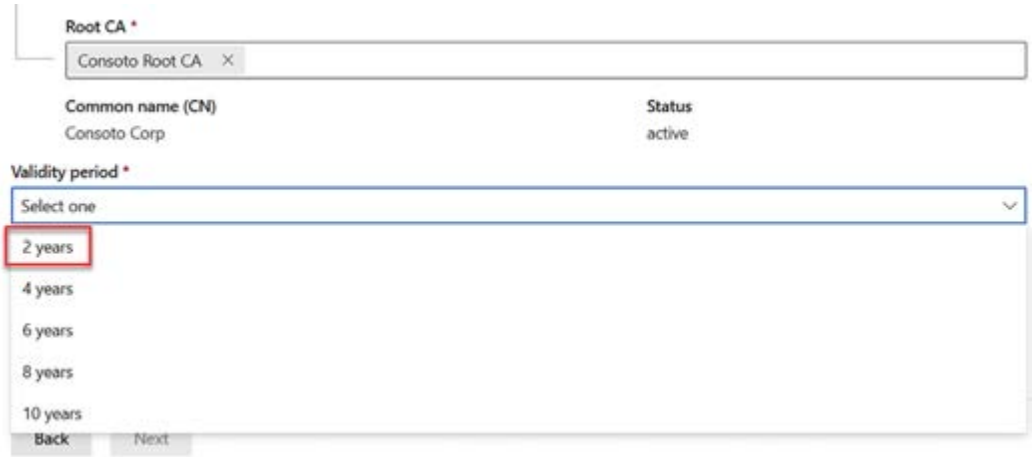


Figure 11.80: Cloud PKI Issuing CA validity period

17. You need to select the **Extended Key Usages** for your new **Issuing CA** that you are creating; only the options that you selected in your **Root CA** are available for selection. In this case, we will select **Client auth** and **Smartcard logon.**



Figure 11.81: Extended Key Usages

18. Then, you can fill out the subject attributes that you want to have in your organization. **Common name (CN)** is the only mandatory attribute.

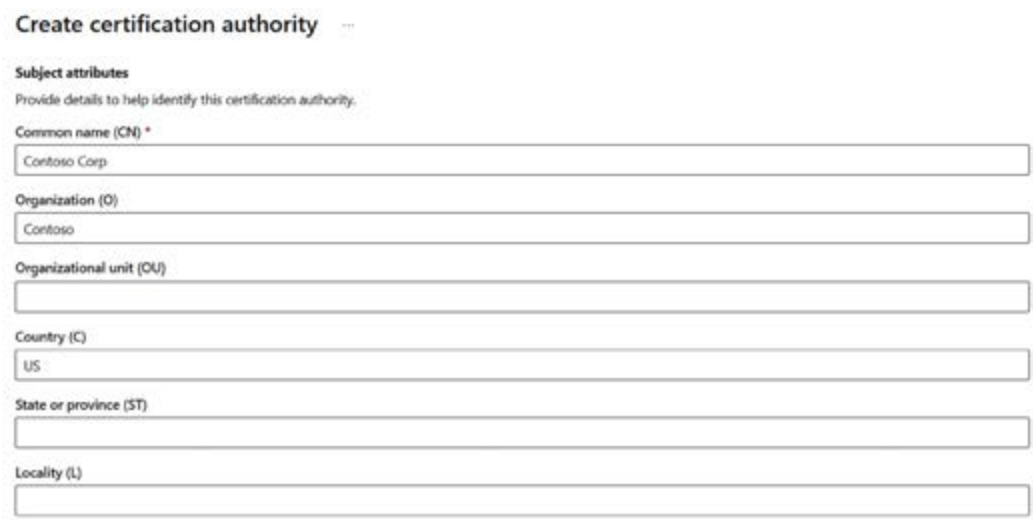


Figure 11.82: Cloud PKI Issuing CA, Subject attributes

As you can see in *Figure 11.83*, the **Encryption** option grayed out on the issuing CA as it will pick the same key size and algorithm that you already selected in the root CA.



Figure 11.83: Cloud PKI Issuing CA, Encryption

19. In the next part of the wizard, you can add **Scope tags** as needed, or just click **Next** to go to the **Review + create** screen.

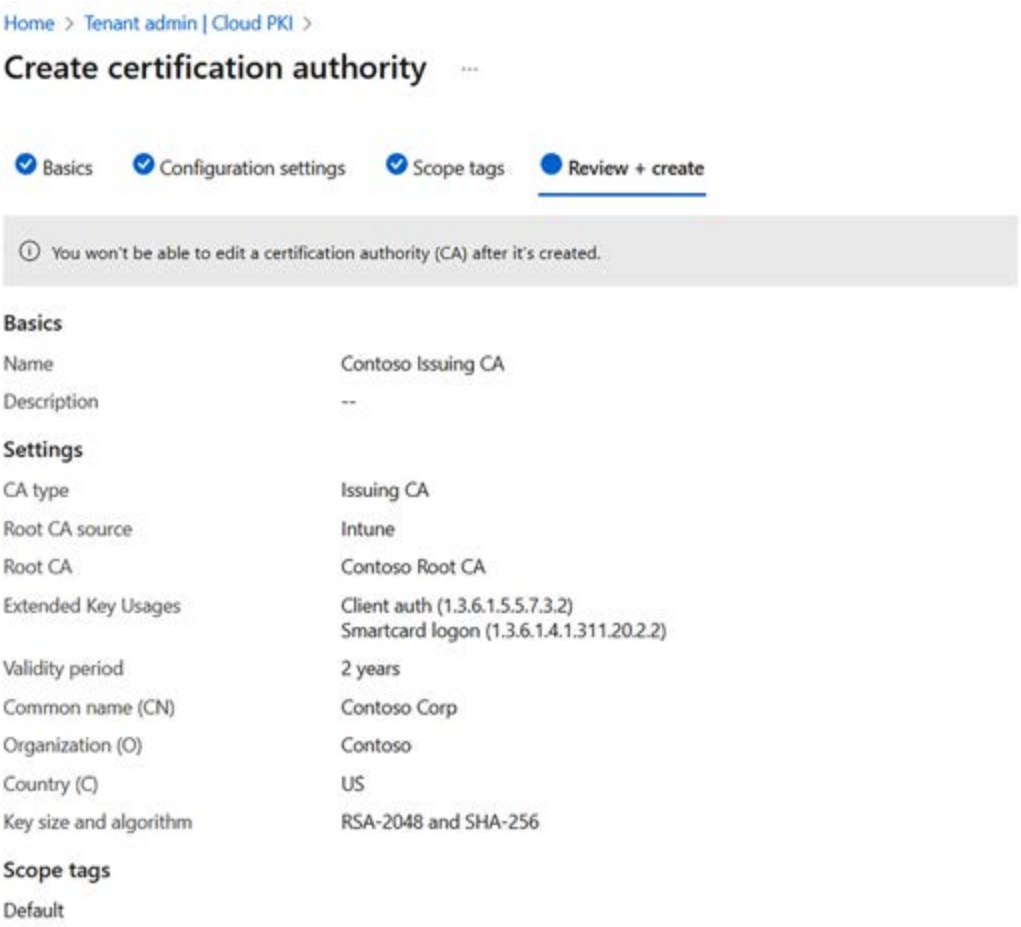


Figure 11.84: Cloud PKI Issuing CA, Review + create

Now you have both the root CA and issuing CA servers deployed for your organization.

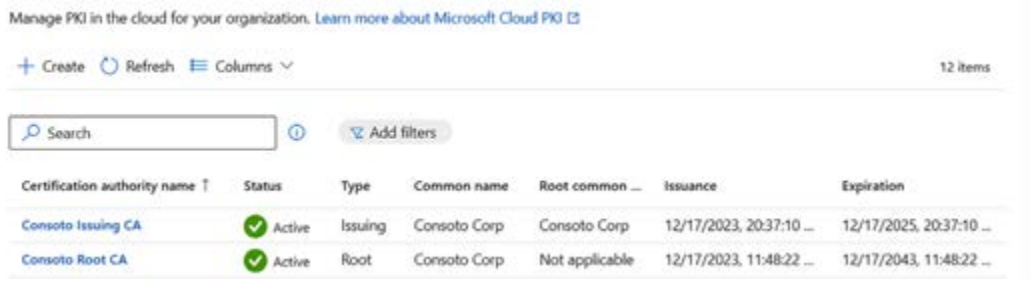


Figure 11.85: Cloud PKI overview

In both the **Root CA** and the **Issuing CA**, you can download the certificate that you need to deploy to your end users' devices.

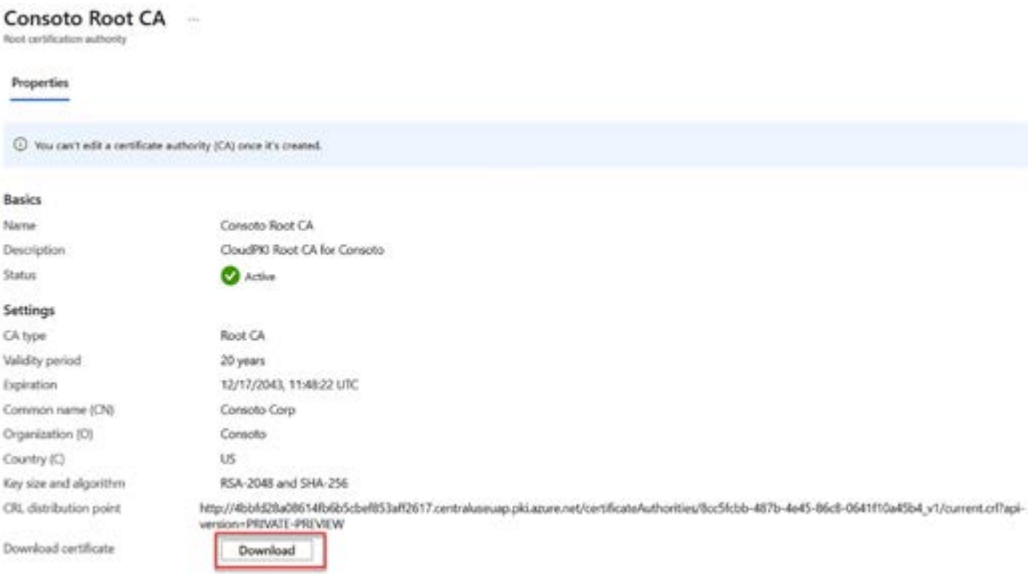


Figure 11.86: Root CA download

You also need to copy the **SCEP URI** from the issuing CA overview as you will need it when creating the SCEP profile in Intune later.

The SCEP URI will be unique for all created issuing CAs.

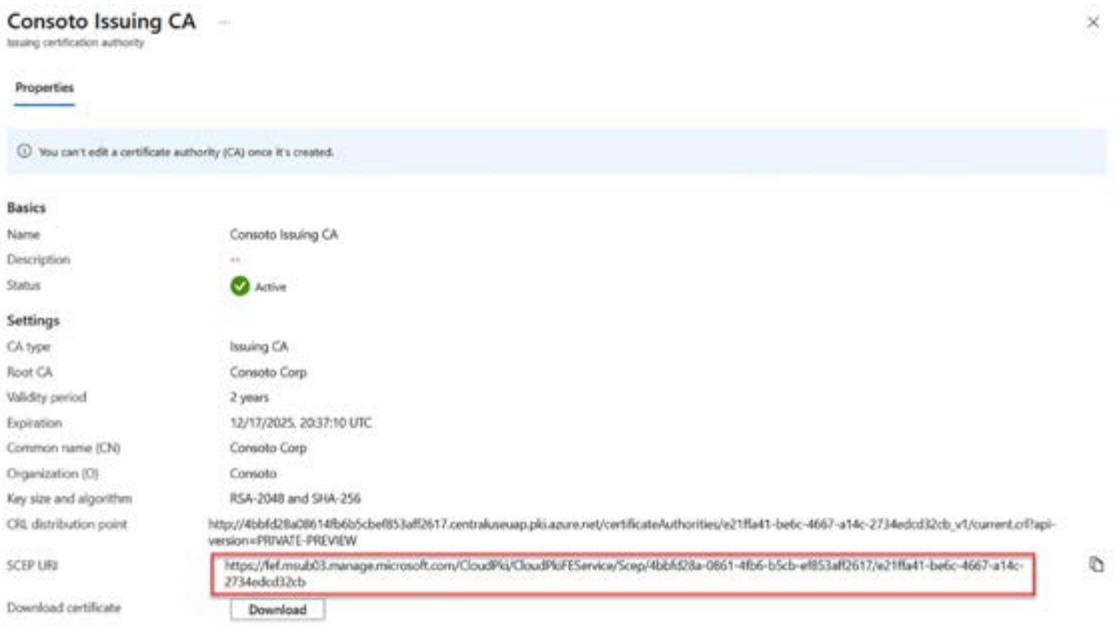


Figure 11.87: SCEP URI

As you can see, the URL for the SCEP URI, **msub03**, matches the tenant location, **Europe 0301**, as the Cloud PKI infrastructure is kept inside your tenant boundaries.



Figure 11.88: Tenant location

Put the root CA and issuing CA files in a location where you can access them easily when you need them later.

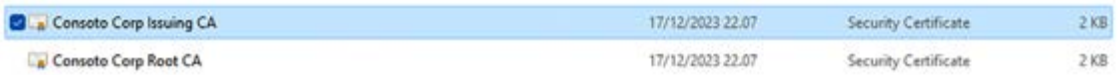


Figure 11.89: Downloaded certificates

This concludes the section on how to set up a cloud-native PKI infrastructure. Now we will walk through certificate revocations.

Certificate Revocation

Certificate revocation is a crucial aspect of enterprise security, even though it might not always be well understood. Let's delve into why we need it and the reasons behind revoking certificates:

Ensuring trust and authentication:

- Digital certificates play a vital role in establishing trust between parties. When we visit a website, our web browser uses certificates to verify that we've arrived at the intended site.
- Certificates are also used for user and device authentication. For instance, smart cards and IoT devices rely on certificates to establish a strong identity.
- To trust a certificate, we need two key security guarantees:
    - **Validity**: Is the certificate created by a trusted authority? Does it have valid start and expiry dates? Does it match the entity providing it?
    - **Revocation status**: Has the certificate been revoked? Revocation ensures that compromised or outdated certificates are no longer trusted.

Reasons for certificate revocation:

- **Affiliation change**: When an individual leaves an organization, changes roles, or the associated computer account is no longer in use.
- **CA compromise**: Suspected compromise of a CA's private key by unauthorized individuals.
- **Certificate hold**: Temporarily suspending a certificate due to ongoing investigations.
- **Cessation of operations**: Revoking certificates when an organization ceases operations.
- **Key compromise**: If a private key is compromised, the certificate must be revoked.
- **Removal from CRL**: Removing a certificate from the **Certificate Revocation List** (**CRL**).
- **Superseded**: Replacing an old certificate with a new one.
- **Unspecified**: Revocation without specifying a reason.

Practical scenarios:

- **Employee changes**: When an employee leaves or changes roles, their certificate should be revoked to prevent unauthorized access.
- **Smart card vulnerabilities**: If vulnerabilities are discovered in smart cards, mass revocation may be necessary.
- **CA breach**: In case the CA itself is compromised; attackers could create valid-looking certificates for malicious purposes.

Remember, certificate revocation ensures that trust remains intact and security risks are minimized. It's a critical part of maintaining a secure digital environment!

If you go to your newly created Issuing CA in the Intune admin center and click on it, you will get an overview of active, expired, and revoked certificates from that issuing CA:

1. Click on **View all certificates**.



Figure 11.90: Issuing CA overview

2. Then select the certificate you want the details on.
3. A new blade pops out, and you can click **Revoke** on that specific certificate.

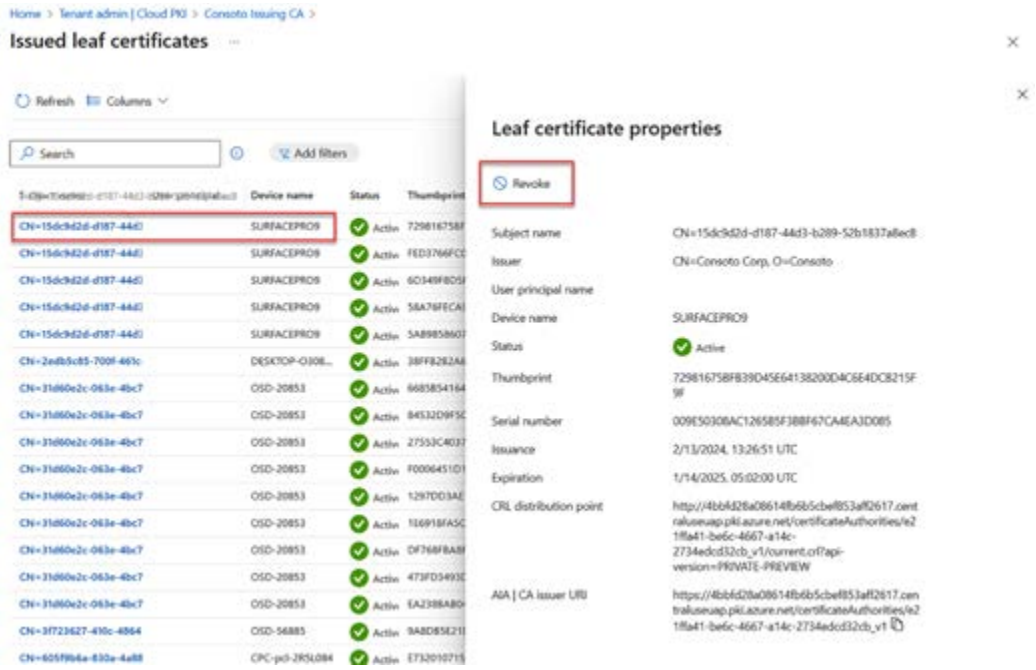


Figure 11.91: Leaf certificate properties

4. You will be prompted with a description of what happens if you revoke the certificate, and you will need to verify that you are okay with this by clicking **Revoke**.

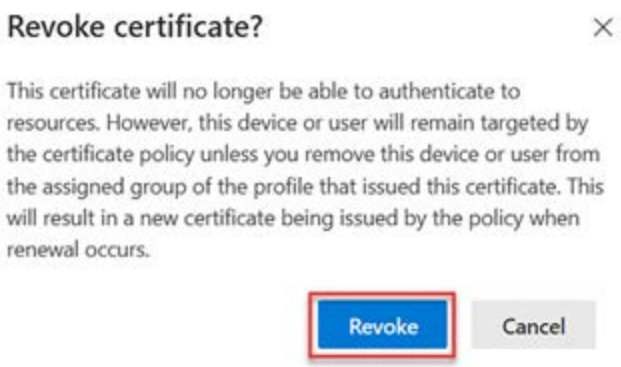


Figure 11.92: Certificate revocation confirmation

This concludes the part about deploying Cloud PKI in your environment.

Now you are ready to deploy the root and issuing certificates for your devices that are managed by Microsoft Intune. As this book covers the Windows management part only, we will only cover that scenario here, but you can leverage the same process for IOS, Android, and MacOS as well.

To configure the Intune profile **trusted certificate** for deployment of the certificates you just created, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Devices** | **Windows** | **Configuration profiles** | **Create Policy**:
    - **Platform**: Select **Windows 10 and later**
    - **Profile type**: **Trusted Certificate**
    - **Name**: **Consoto Root CA**



NOTE

Import the trusted root certificate from your CA and assign it to devices that use SCEP and PCKS certificates to authenticate within your organization's resources.

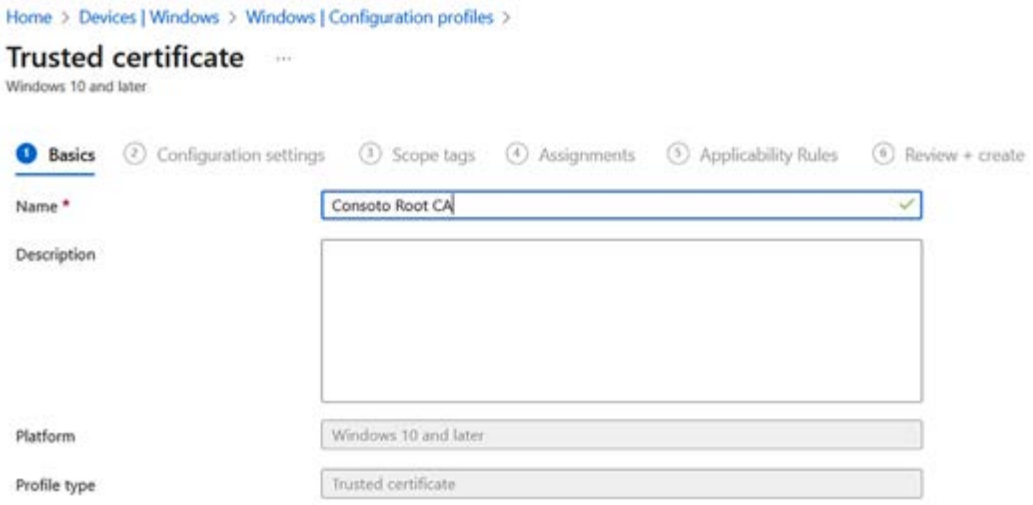


Figure 11.93: Trusted certificate Root CA

2. Upload the Root CA that you downloaded earlier.
3. For Destination store, select **Computer certificate store – Root**.

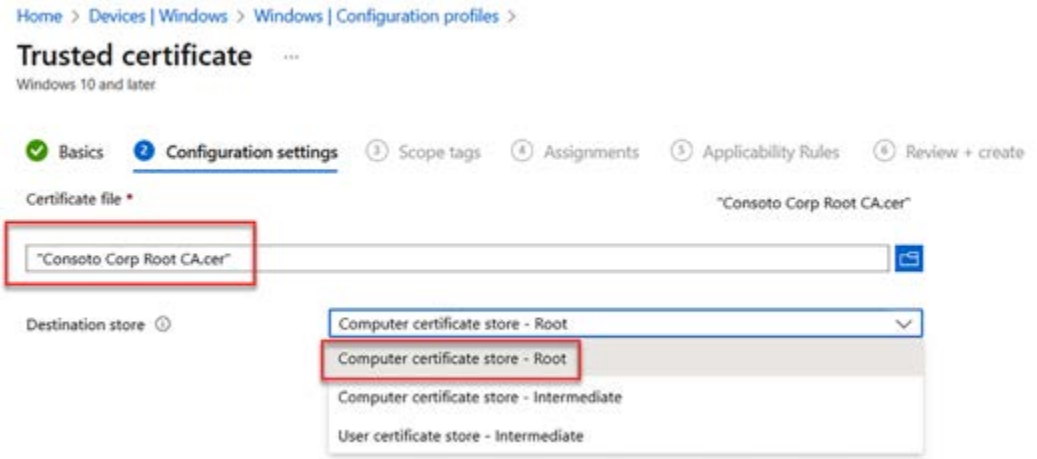


Figure 11.94: Trusted certificate Root CA, Configuration settings

4. Click **Next** and add a **scope tag** (if needed).
5. Click on **+ Add all devices** to assign to all devices.

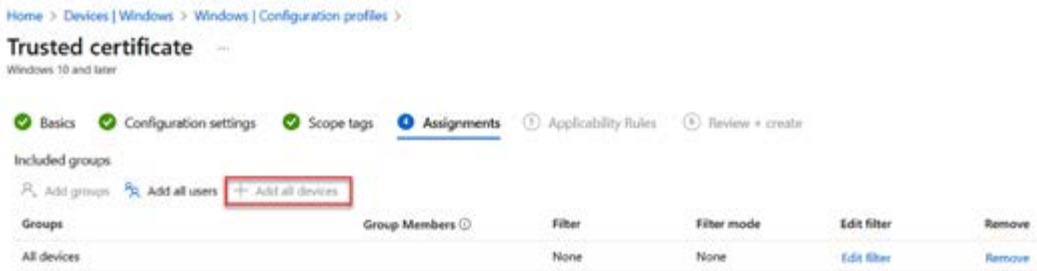


Figure 11.95: Trusted certificate Root CA assignment

6. Click **Next.**
7. In **Applicability Rules**, click **Next.**
8. In **Review + create**, click **Create**
9. Redo the same steps for the issuing CA.

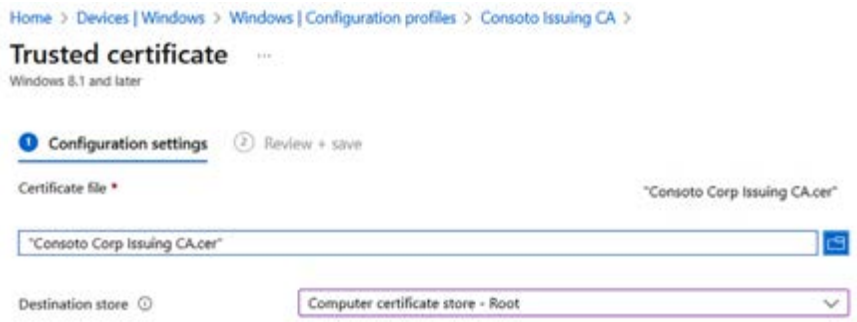


Figure 11.96: Trusted certificate Issuing CA configuration settings

After the next **Mobile Device Management** (**MDM**) sync, the Windows client will receive the trusted root certificate that you have just deployed.

For troubleshooting, you can go into the trusted certificate policy you just created and verify that it has succeeded and no errors are listed.

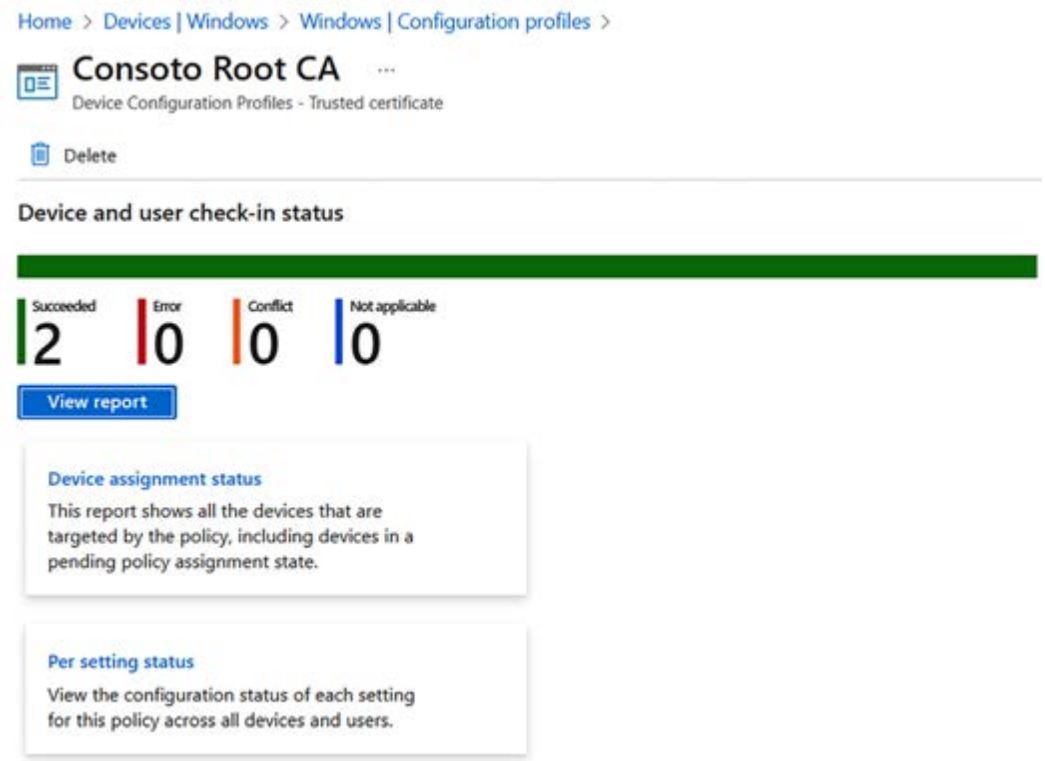


Figure 11.97: Trusted certificate overview

You can click on **View report** and get more detailed information about where the certificate has been deployed to:

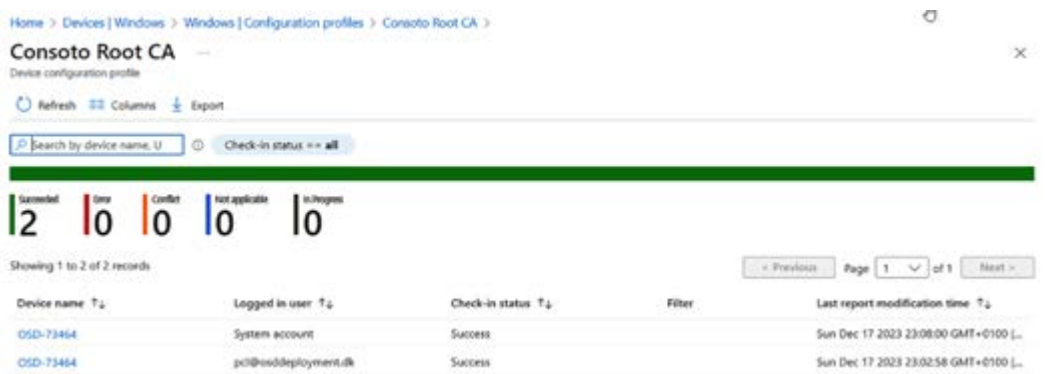


Figure 11.98: Trusted certificate device report details

Start Command Prompt on your Windows client and type `certlm.msc` to start the Certificates snap-in in the **Microsoft Management Console** (**MMC**).



Figure 11.99: certlm.msc

Now you have deployed the root certificate to your devices. Next, you can deploy the user or device certificate, and we are using SCEP certificate profiles for that.

Now you need to create the Intune SCEP certificate profile:

1. In the Microsoft Intune admin center, go to **Home** | Devices | **Windows | Configuration profiles | Create** | **New Policy**:
    - **Platform**: Select **Windows 10 and later**
    - **Profile type: SCEP certificate**
    - **Name: Consoto SCEP certificate**

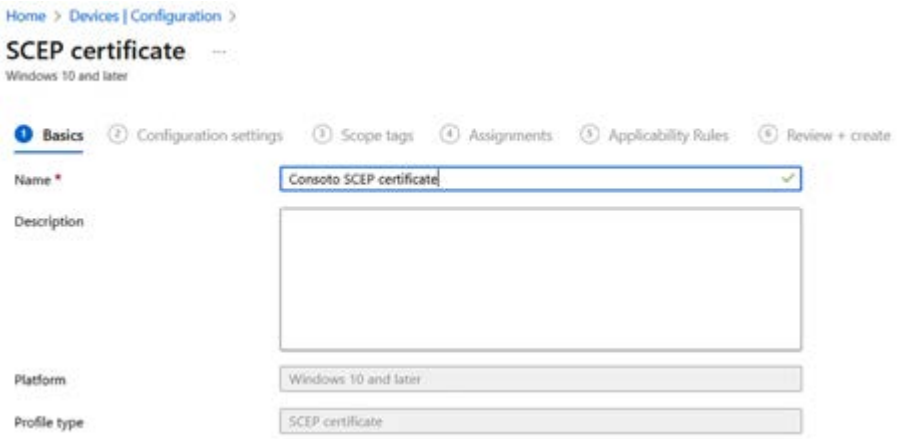


Figure 11.100: SCEP Certificate profile basics

2. Click **Next**.
3. In the **Configuration settings**, you need to select the certificate type. Here, select either **User** or **Device** from the drop-down menu.

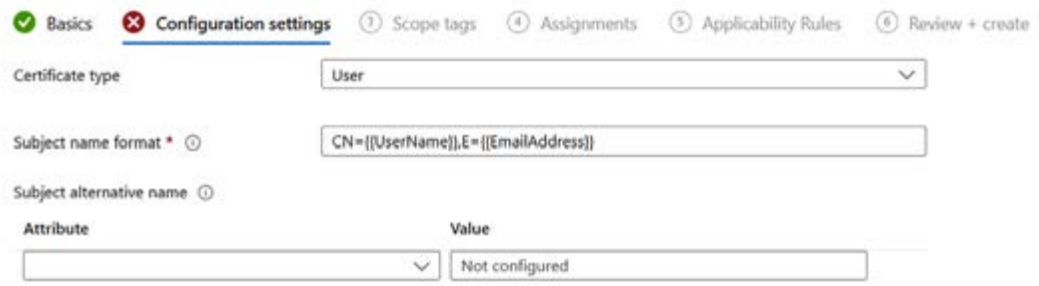


Figure 11.101: SCEP Certificate profile configuration settings

4. In **Subject name format**, **Common Name (CN)** can be set to any of the following variables:
   - `CN={{UserName}}`: The user name of the user, such as `perlarsen`.
   - `CN={{UserPrincipalName}}`: The user principal name of the user, such as `pcl@osddeployment.dk`.
   - `CN={{AAD_Device_ID}}`: An ID assigned when you register a device in Microsoft Entra ID. This ID is typically used to authenticate with Microsoft Entra ID.
   - `CN={{SERIALNUMBER}}`: The unique **Serial Number** (**SN**) typically used by the manufacturer to identify a device.
5. User certificates use `CN={{UserName}},E={{EmailAddress}}` – if the user does not have an email address in Entra, the certificate will not be issued to the user and an error will be shown in the SCEP certificate profile report.

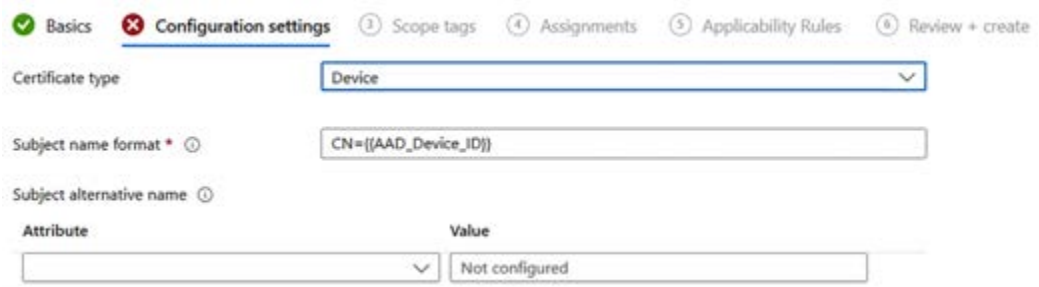


Figure 11.102: SCEP certificate profile configuration settings

6. If you select **Device** for **Certificate type**, it will be issued to the device.
7. You need to enter the certificate validity period from 1 to 5 years or choose months or days. Shorter-lived certificates reduce the window of vulnerability. If a certificate's private key is compromised, it remains valid for a shorter duration, minimizing the impact.

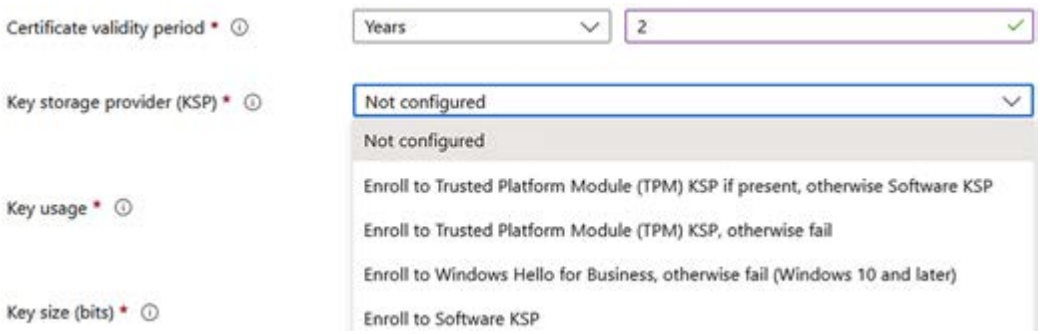


Figure 11.103: SCEP certificate profile key storage provider

8. You need to specify the **Key storage provider (KSP)** option as the following, as shown in the preceding figure:
    - **Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP**
    - **Enroll to Trusted Platform Module (TPM) KSP, otherwise fail**
    - **Enroll to Windows Hello for Business, otherwise fail (Windows 10 and later)**
    - **Enroll to Software KSP**

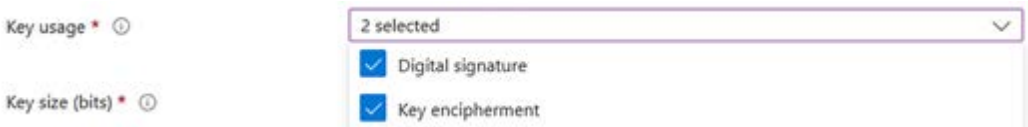


Figure 11.104: SCEP certificate profile key usage

9. Select the following options for the **Key** usage option, as shown in the preceding figure:
    - **Digital signature:** Allows key exchange only when a digital signature helps protect the key.
    - **Key encipherment:** Allows key exchange only when the key is encrypted.

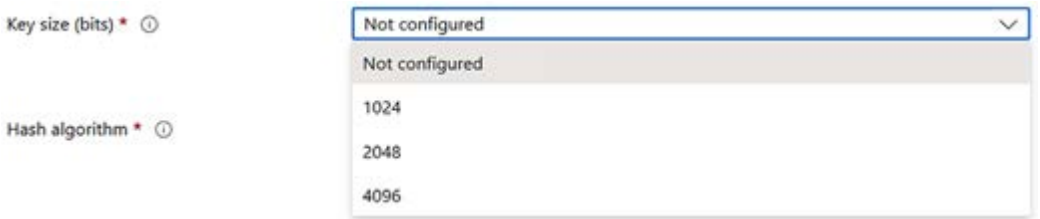


Figure 11.105: SCEP certificate profile key size

10. Select the following options for the **Key size** (**bits**) dropdown, as shown in the preceding figure:
    - **Not configured**
    - **1024**

- **2048**
- **4096**

Hardware-based TPMs do not support 4096-bit keys, so if you want to leverage 4096-bit keys, you need to configure the storage provider to allow a software **Key Storage Provider** (**KSP**).

Windows Hello for Business does not currently support 4096-bit certificates and there is no workaround at the time of writing this book. You can get the most updated information in the public Microsoft docs for Windows Hello for Business at `https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/deploy/#pki-requirements`.

For the hash algorithm, use SHA-2 if possible, as Microsoft stopped using SHA-1 for signing TSL certs, code-signing, and file hashing back in 2021. Do not use SHA-1 certificates unless your particular infrastructure relies on that certificate format and cannot handle the newer SHA-2 hash algorithm.



Figure 11.106: SCEP certificate profile hash algorithm

11. Select **Root Certificate**.



Figure 11.107: SCEP certificate profile Root CA

12. Select the **Root CA**, as the Cloud PKI service is a multi-tier PKI infrastructure, so selecting the top-level trusted root CA will validate the issuing CA as well.



Figure 11.108: SCEP certificate profile Root CA

13. Select **Client Authentication** in **Predefined values**.



Figure 11.109: SCEP certificate Client Authentication

14. Previously, you copied the **SCEP URI**, and now you can paste it into the SCEP certificate profile.

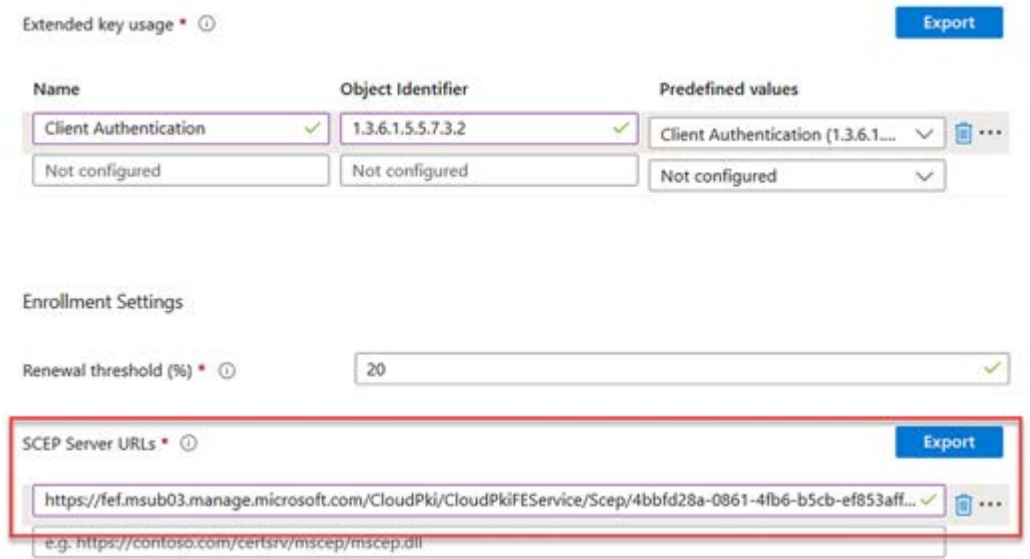


Figure 11.110: SCEP certificate profile SCEP Server URL

15. Click **Next** in **Scope tags**.
16. Click **Add all devices** or **Add all users** depending on whether it is a user or a device certificate profile you have just created. You can also assign it to a scoped Entra user or device group as per your requirements.
17. Click **Next** in **Applicability Rules**.
18. Click **Create** in **Review + create**.

Your users or devices will receive the certificate on the next MDM sync.

Now you can start to leverage the certificates for Wi-FI, VPN, and so on by creating a new template profile in Intune and deploying it to your devices.

To read more about certificates, visit these links:

- *Securing PKI: Planning Certificate Algorithms and Usages*: `https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786428(v=ws.11)`
- *NIST SP 800-57 Part 1 Rev. 5 – Recommendation for Key Management: Part 1 – General*: `https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final`

This concludes the section on Cloud PKI. We will continue with Remote Help for Windows.

Remote Help for Windows

Microsoft Intune provides a cloud-based solution called Remote Help for secure help desk connections with role-based access controls. With the connection, your support staff can remotely connect to the user's device. During the session, the support staff can view the device's display and, if permitted by the device user, take full control. Full control enables a helper to directly make configurations or take actions on the device. Remote Help uses Intune **role-based access control** (**RBAC**) to set the level of access a helper is allowed. Through RBAC, you determine which users can provide help and the level of help they can provide. The Remote Help app is available from Microsoft to install on devices enrolled with Intune and devices that aren't enrolled with Intune. The app can also be deployed through Intune to your managed devices.

The Remote Help app supports conditional access, compliance warnings, and elevation of privilege.

As this book is all about Windows management, in this section on Remote Help, we will also focus on Remote Help for Windows. Remote Help does support Android and macOS as well, but we will not cover those platforms here.

How to enable Remote Help

Included in the different Remote Help license solutions (standalone or Intune Suite), you also have integration with ServiceNow, which allows helpdesk administrators to view user-submitted ServiceNow incidents in the Troubleshooting blade. We will not cover that integration in this book.

To configure Remote Help in Intune, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Tenant administration** | **Remote Help** | **Settings** | **Configure**:

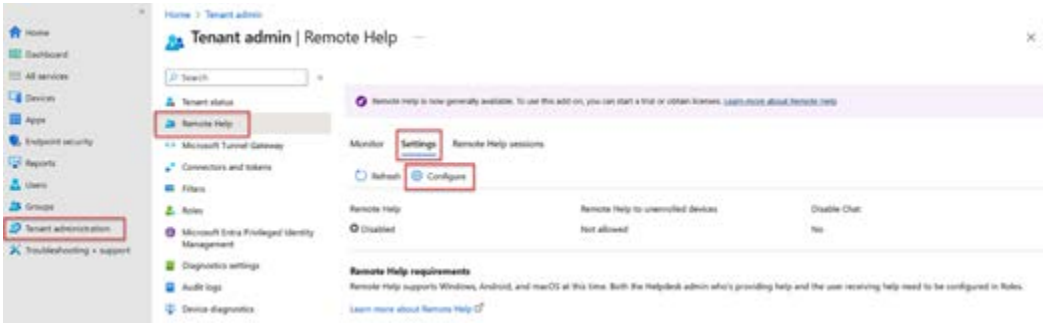


Figure 11.111: Remote Help Configure

Configuring Remote Help in Intune

We recommend you configure Remote Help with the following settings:

- **Enable Remote Help: Enabled.** This enables Remote Help for managed devices to be initiated from Microsoft Intune.
- **Allow Remote Help to unenrolled devices: Allowed.** For Windows and macOS devices, enabling this option will allow help for devices that aren't enrolled with Intune.
- **Disable Chat: No**

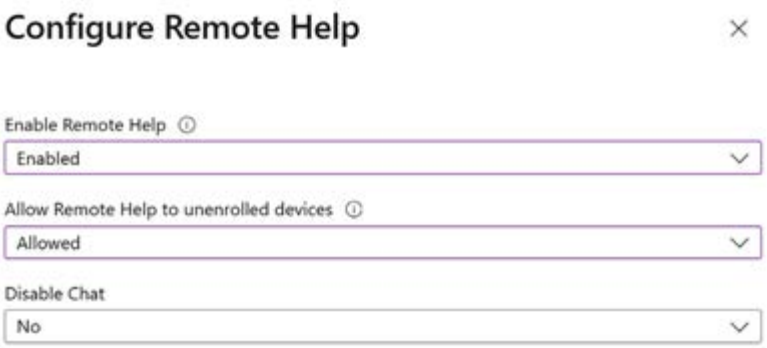


Figure 11.112: Configure Remote Help

You can always change these settings later if your organization's requirements change.

Before you can leverage Remote Help for an Intune-managed device, you need to download the Remote Help client from `https://aka.ms/downloadremotehelp`, package the Remote Help client as a Win32 app, and upload it in Intune.

If you have the license for Enterprise App Management, you can also add Remote Help as an **Enterprise App catalog** app.

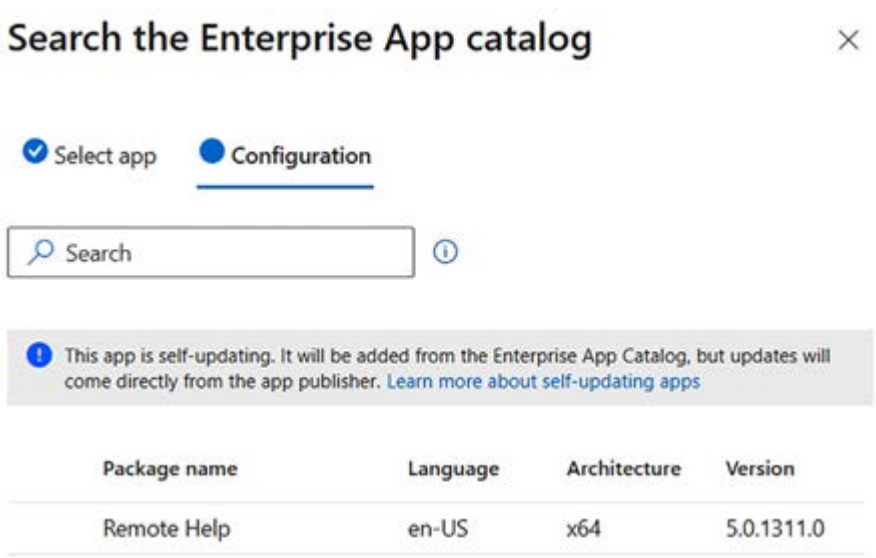


Figure 11.113: Remote Help app

In *Chapter 8*, we showed you how to create and deploy packages for Win32 applications:

- **Install command line:** `remotehelpinstaller.exe /quiet acceptTerms=1`
- **Uninstall command line:** `remotehelpinstaller.exe /uninstall /quiet acceptTerms=1`

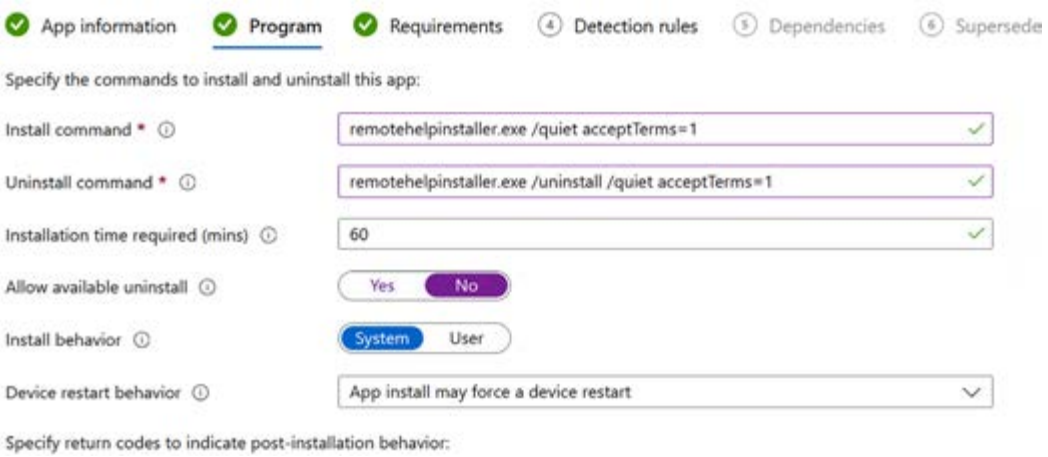


Figure 11.114: Remote Help Win32 app

Remote Help will automatically be updated once you have installed it on your Windows devices.

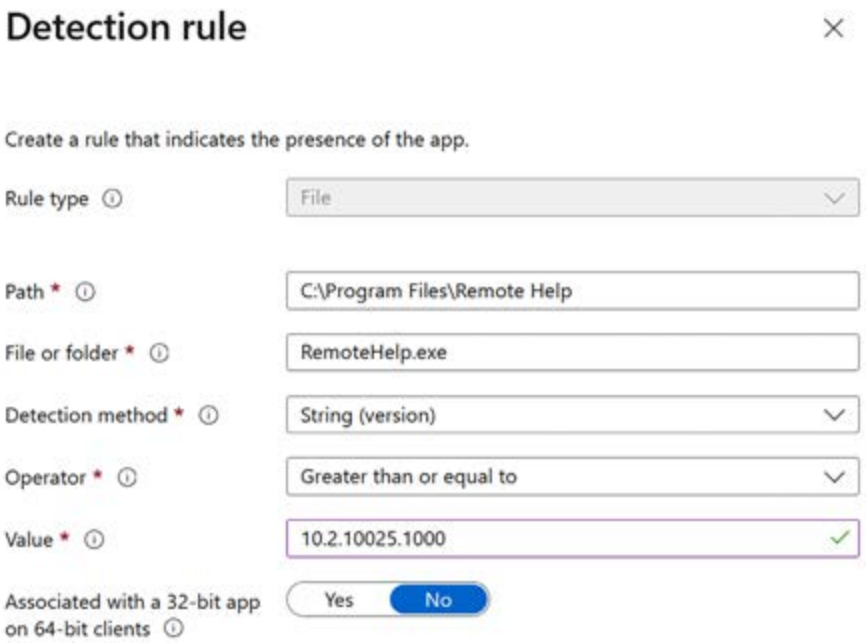


Figure 11.115: Remote Help Win32 app detection rule

Create a detection rule like this for the Win32 app, as shown in the preceding figure:

- **Rule type:** `File`
- **Path:** `C:\Program Files\Remote Help`
- **File or folder:** `RemoteHelp.exe`
- **Detection method:** `String (version)`
- **Operator:** `Greater than or equal to`
- **Value:** `10.2.10025.1000`

Now you just need to deploy it to a user or device group.

This concludes the section on how to install Remote Help on your end users' devices. Now we will take a look at how the Remote Help experience looks from an end user's perspective.

How does Remote Help look from an end user's perspective?

Let's understand this with these steps:

1. End users will see a Remote Help window and will be able to sign in with their Entra ID credentials.

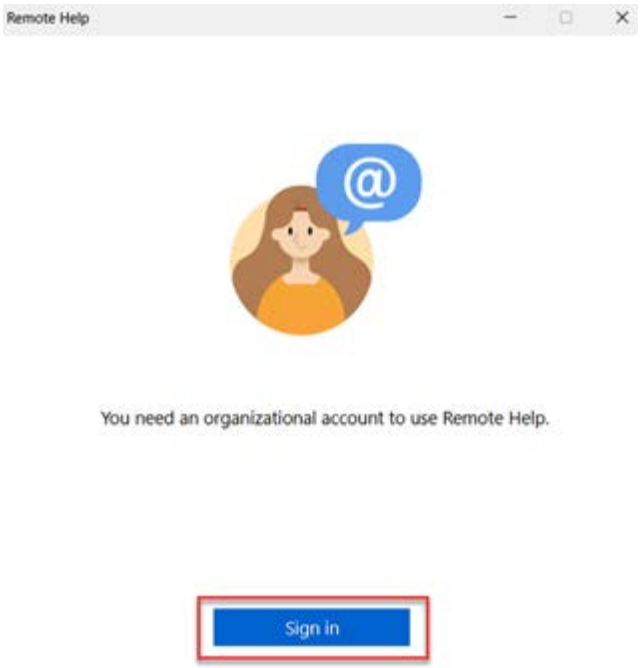


Figure 11.116: Remote Help Sign in screen

2. The end user will be asked to accept the privacy terms.

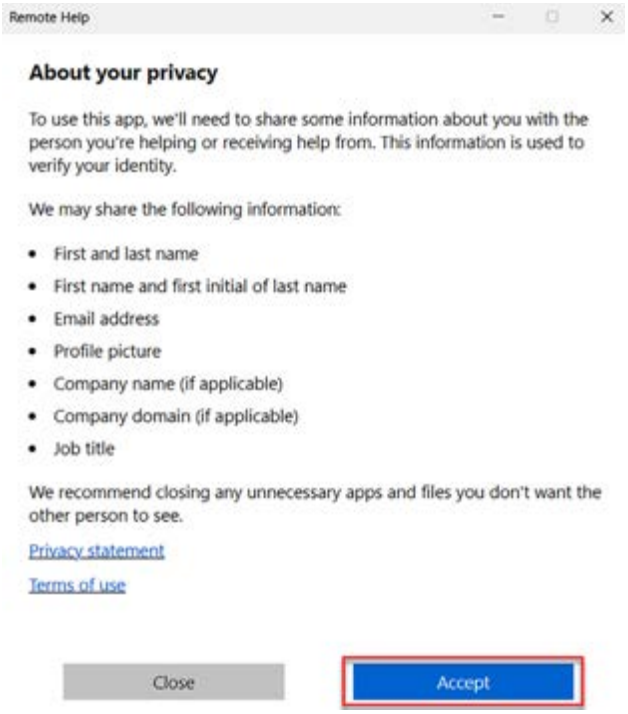


Figure 11.117: Remote Help About your privacy

3. After signing in to Remote Help with their credentials, they can enter the security code from their helper or service desk in the field provided.

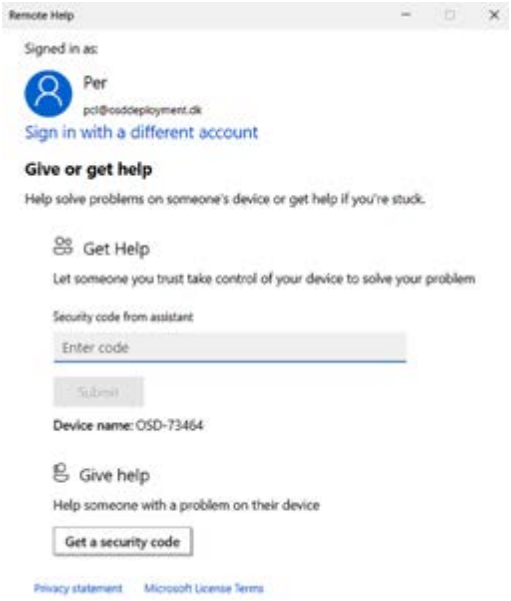


Figure 11.118: Remote Help Windows app

How do you remotely access a managed device?

To remotely access a managed device, follow these steps:

1. As an IT administrator with the correct RBAC permissions for remote control using Remote Help, you find the end user's device, hit the three dots (**...**), and click **New remote assistance session**.

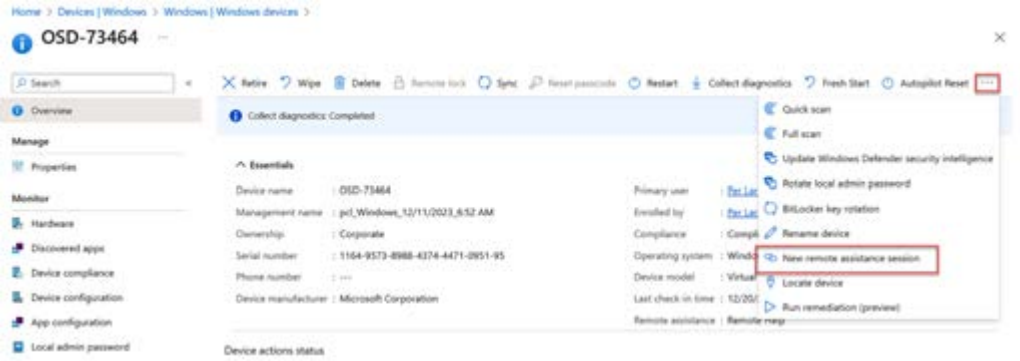


Figure 11.119: New remote assistance session

2. The IT admin needs to click **Continue** when they have verified that it is the right device they are trying to get remote access to.

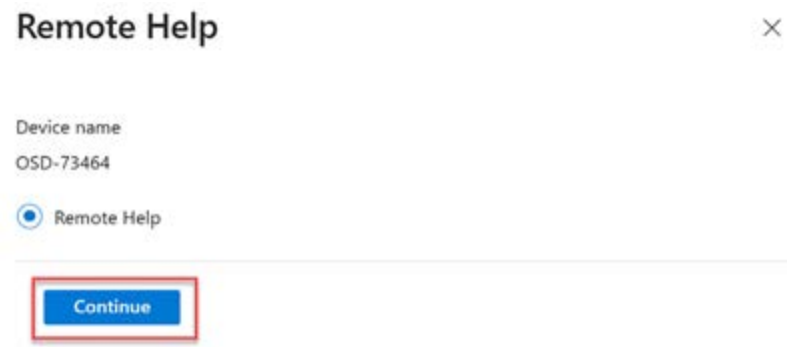


Figure 11.120: Remote Help session

3. An end user toast notification in the Windows regional language will show up for the end user, and they can click **Open Remote Help**.

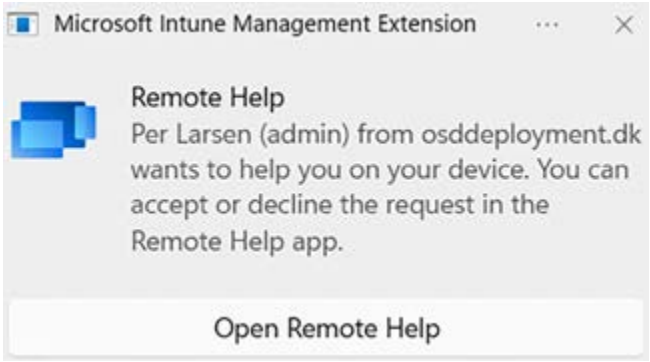


Figure 11.121: Remote Help Windows toast notification

4. When Remote Help is opened on the end user's device, the end user can see the name and picture of the person who wants to remotely access their device.

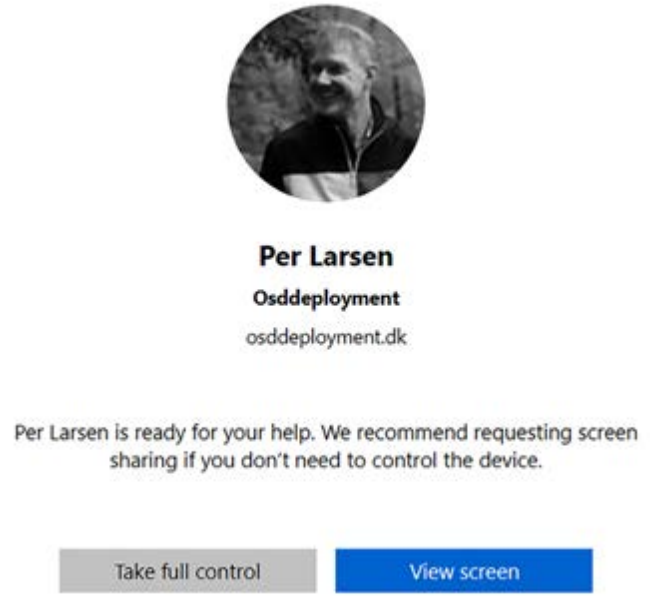


Figure 11.122: Remote Help Windows remote control

5. The end user needs to select either **Take full control** or **View screen** before the IT admin gets access to the device.

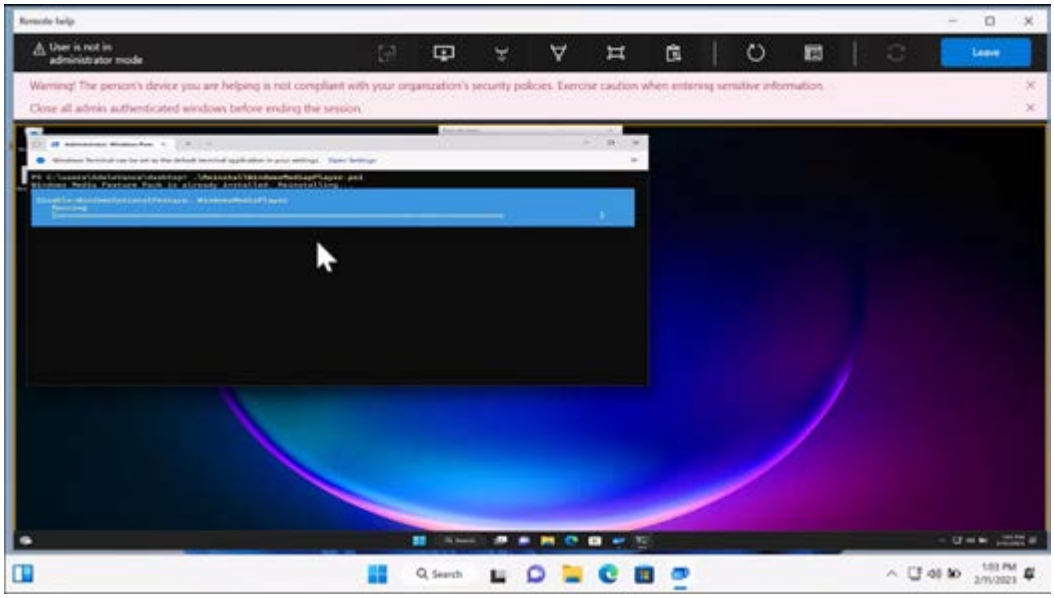


Figure 11.123: Remote Help full control

This concludes the section on how the end user experience looks with Remote Help. In the next section, we will walk through how to configure the local Windows Firewall for Remote Help.

Remote Help Windows Firewall setup

Depending on your Windows Firewall configuration, sometimes, you may need to create firewall rules to allow the Remote Help executable through the Windows Firewall:

- `C:\Program Files\Remote help\RemoteHelp.exe`
- `C:\Program Files\Remote help\RHService.exe`
- `C:\Program Files\Remote help\RemoteHelpRDP.exe`

To configure a Windows Firewall Rules policy, follow these steps:

1. In the Microsoft Intune admin center, go to **Home | Endpoint Security | Firewall | Create Policy:**

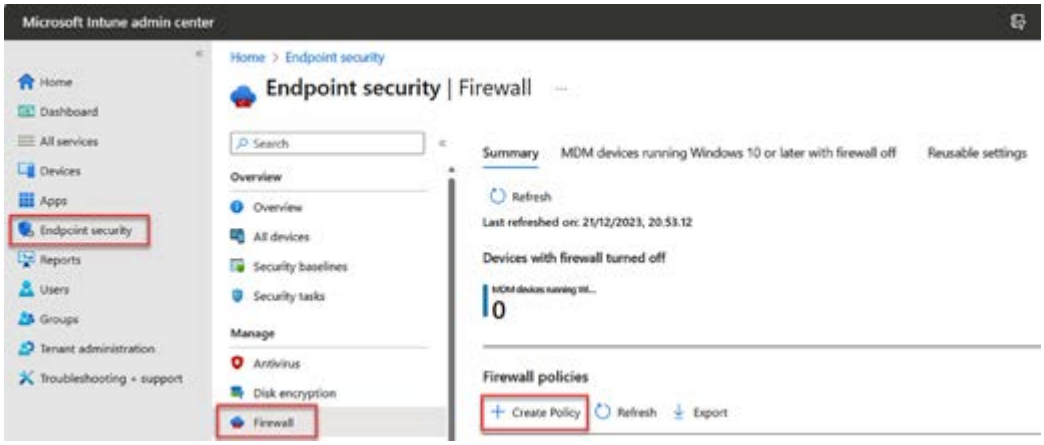


Figure 11.124: Remote Help Windows Firewall

2. For **Platform**, select **Windows 10, Windows 11, and Windows Server.**
3. For **Profile**, select **Windows Firewall Rules.**

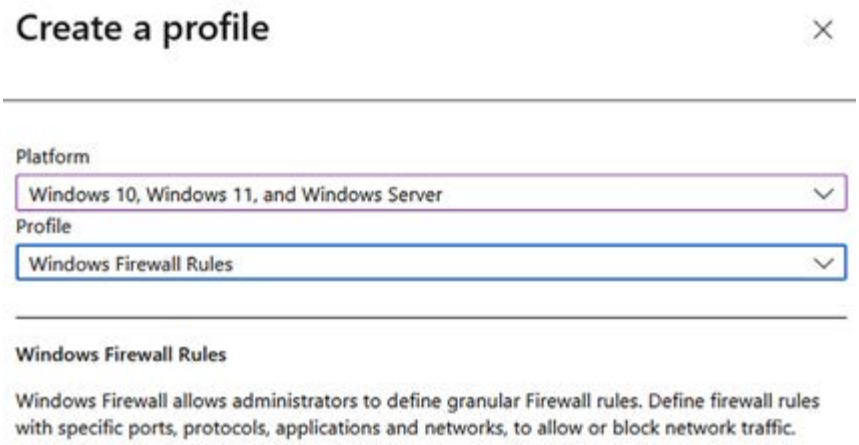


Figure 11.125: Remote Help Windows Firewall Rules policy

4. Give the policy a name: `Remote Helper`.

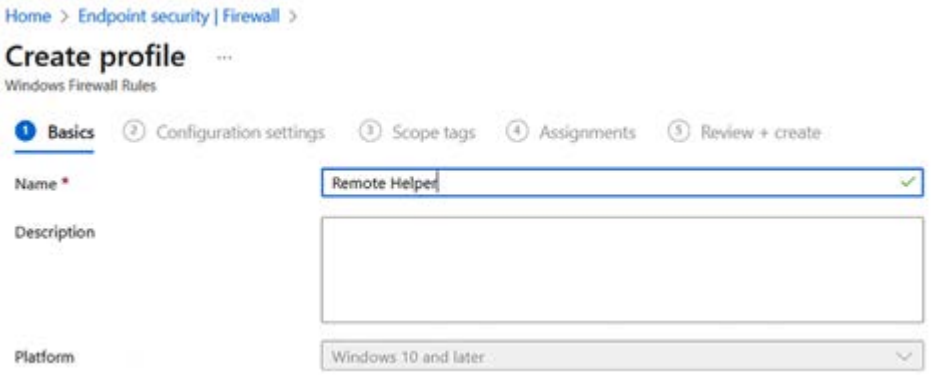


Figure 11.126: Windows Firewall Rules policy name

5. Configure the instance under **Configuration settings:**

   - **Enabled: Enabled**
   - **Name:** `RemoteHelp`
   - **Interface Types: All**
   - **File Patch:** `C:\Program Files\Remote help\RemoteHelp.exe`
   - **Network Types:** Select all applicable
   - **Direction:** The rule applies to inbound traffic

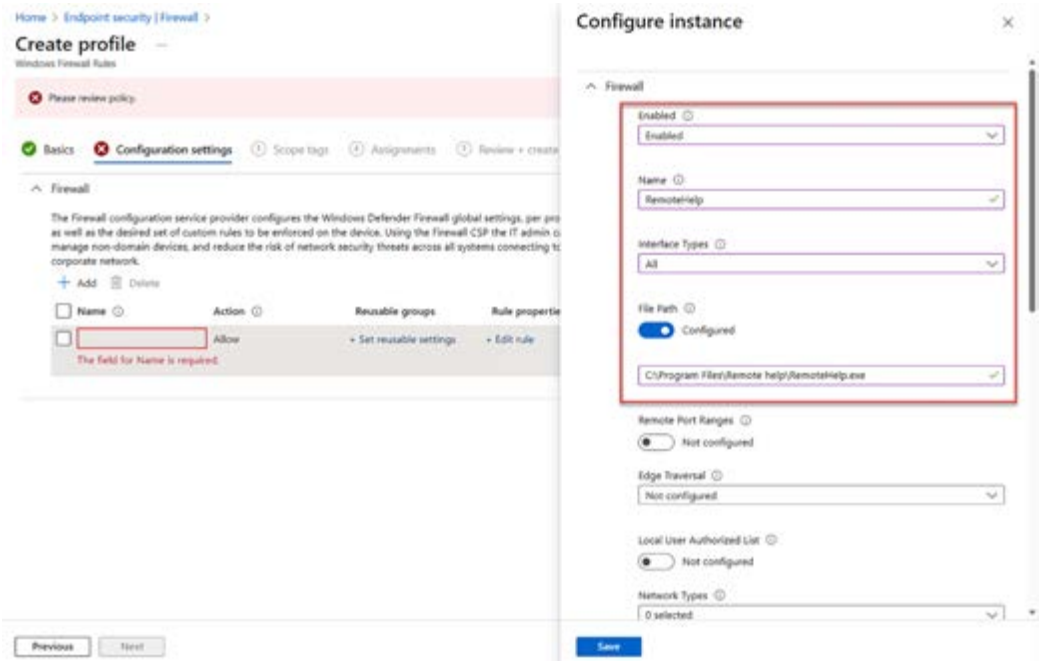


Figure 11.127: Windows Firewall Rules Configure instance

6. Create two more firewall rules for file path for the three files listed at the start of this section.
7. Now you have three rules in your Windows Firewall Rules policy.

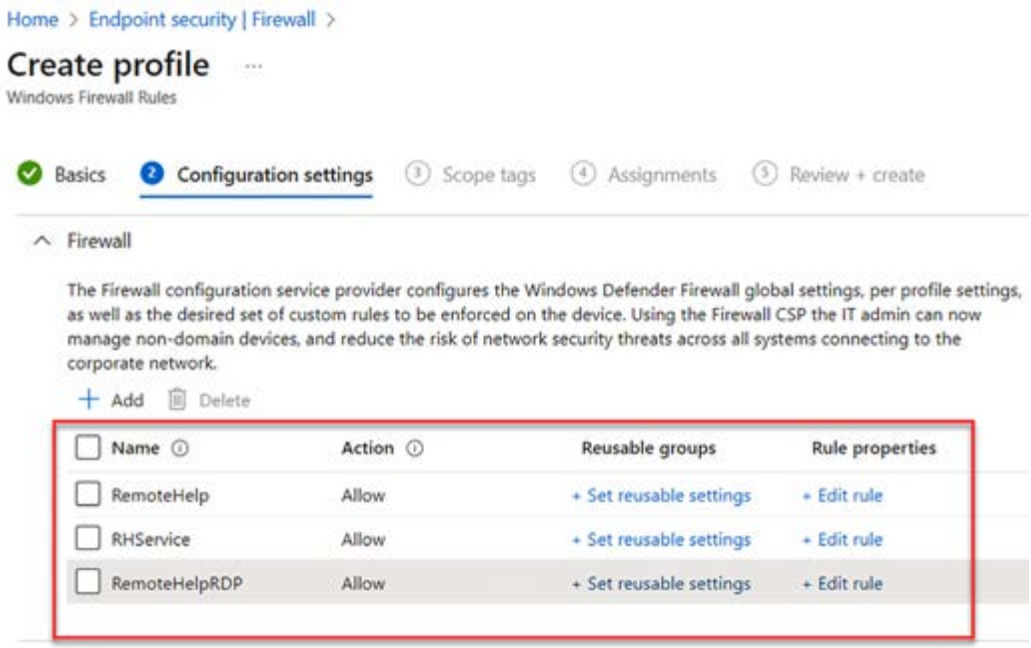


Figure 11.128: Windows Firewall Rules configuration settings

Deploy the Windows Firewall Rules policy to a group of devices or all devices.

Conditional Access for Remote Help

Before you configure Conditional Access for Remote Help, you need to create an app that you can leverage in Entra. The following are the steps you need:

1. Start PowerShell as an administrator, and run these commands:

```
Install-Module Microsoft.Graph -force
Connect-MgGraph: enter your global admin credentials.
```

2. Create a new service principal for RemoteAssistanceService:

```
New-MgServicePrincipal -AppId "1dee7b72-b80d-4e56-933d-8b6b04f9a3e2"
```

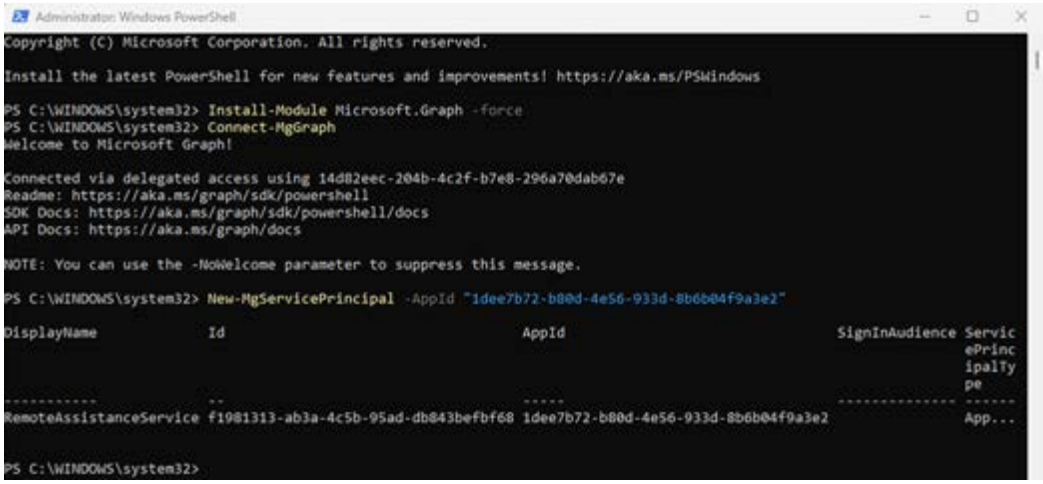


Figure 11.129: Service principal for RemoteAssistanceService

Now you can configure Conditional Access for Remote Help by accessing the Microsoft Entra admin center at `https://entra.microsoft.com/`.

To configure Conditional Access for Remote Help, follow these steps:

1. In the Microsoft Entra admin center, go to **Protection** | **Conditional Access** | **Create new policy**:

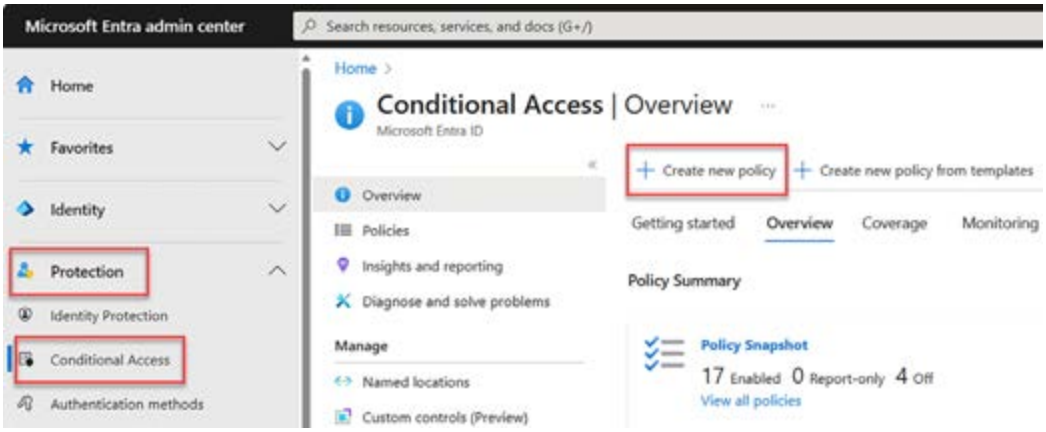


Figure 11.130: Conditional Access

2. Use the following settings:

   Users: All users (maybe exclude a specific group)

   - **Name:** `Conditional Access for Remote Help`
   - **Target resources**
   - **Select apps:** Search for `RemoteAssistanceService`

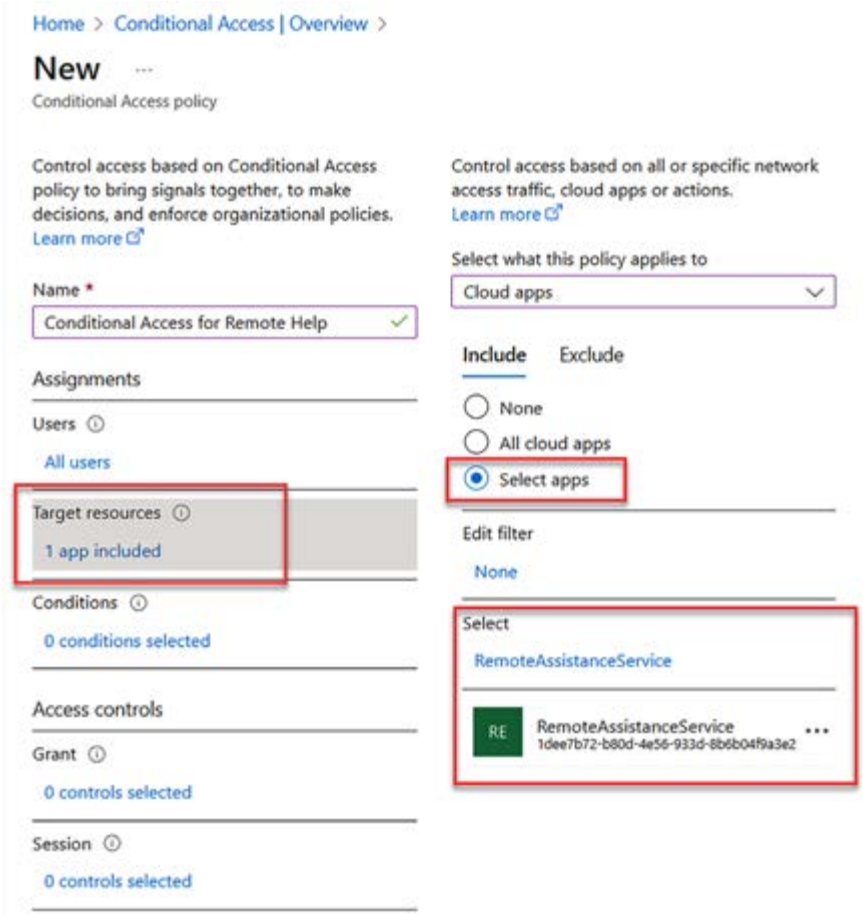


Figure 11.131: Conditional Access – RemoteAssistanceService



NOTE

If you are not able to find RemoteAssistanceService, then you have not completed the previous task (check **Conditional Access for Remote Help**) by creating the new service principal name for RemoteAssistanceService.

3. Click **Conditions.**

4. In **Device platforms**, select **Windows**.

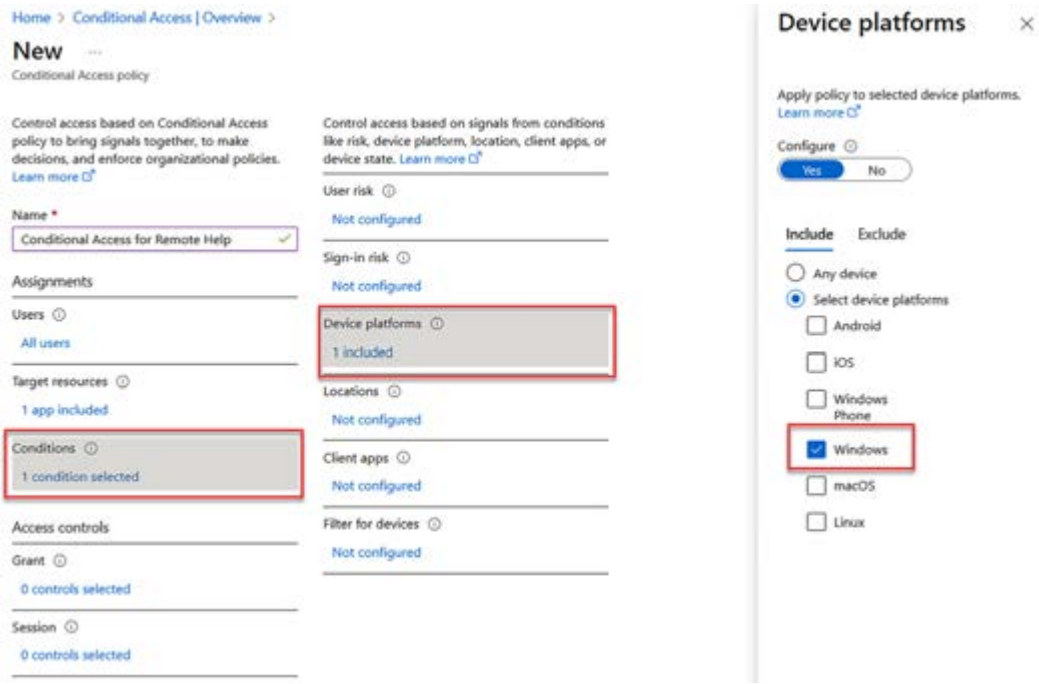


Figure 11.132: Conditional Access – Device platforms

5. You can configure the policy so that the IT admin that is remotely accessing an end user's device requires authentication strength.
6. Click **Grant.**

7. For **Grant access**, select **Require authentication strength** and set it to **Passwordless MFA.**

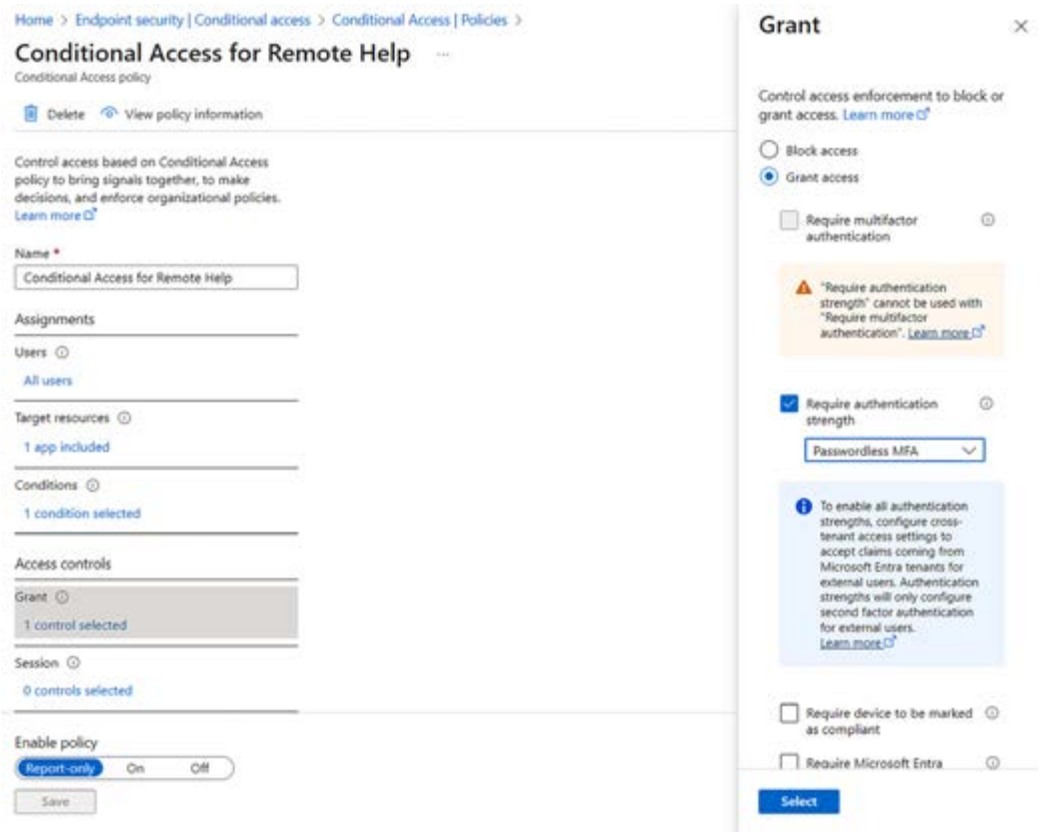


Figure 11.133: Conditional Access – Grant if passwordless

8. You can also configure it so that the IT admin that is remotely accessing an end user's device requires a compliant device – those two can also be configured to **Require one of the selected controls.**

9. Click **Grant.**
10. For **Grant Access**, select **Require device to be marked as compliant.**

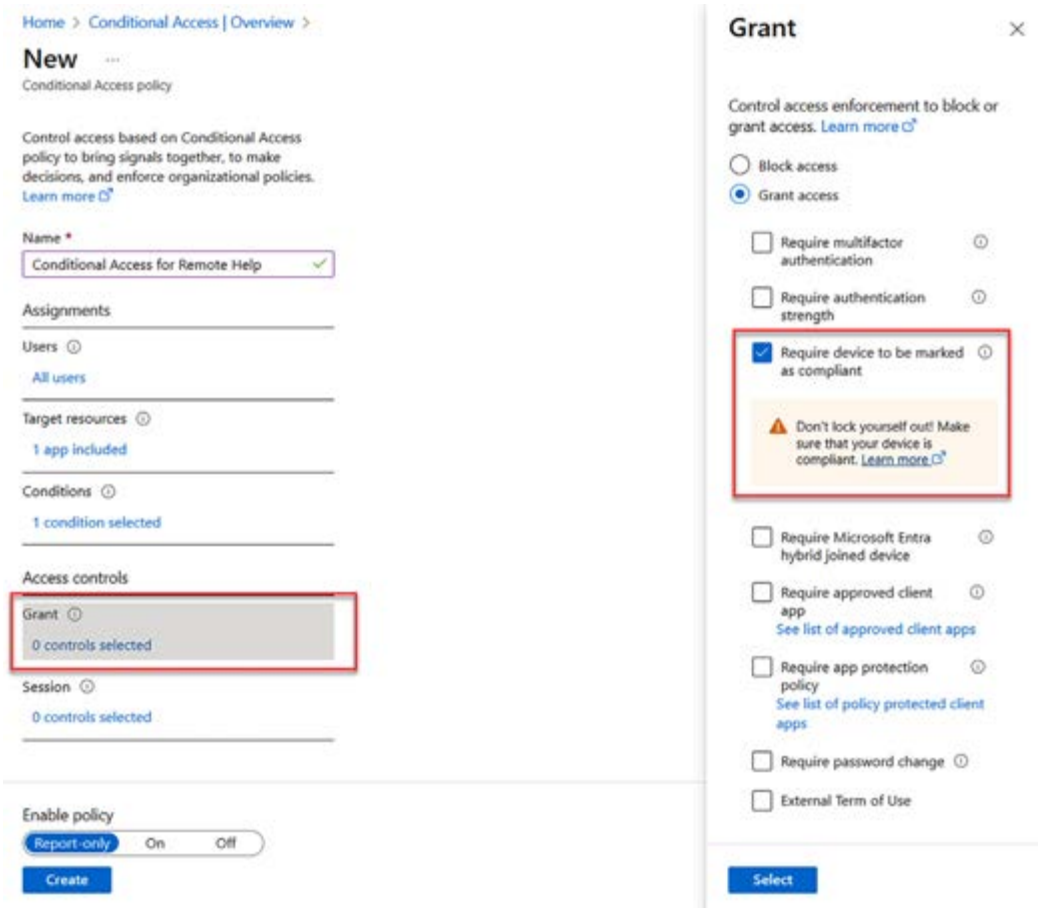


Figure 11.134: Conditional Access – Grant if compliant device

11. Then you need to set **Enable policy** to **On** for the policy to have effect.



Figure 11.135: Set Enable policy to On

How to use Remote Help as an end user and as a ServiceDesk user

If you do not have a Remote Help license in your tenant, all settings will be grayed out, and you will not be able to enable this ability until the required licenses are procured.

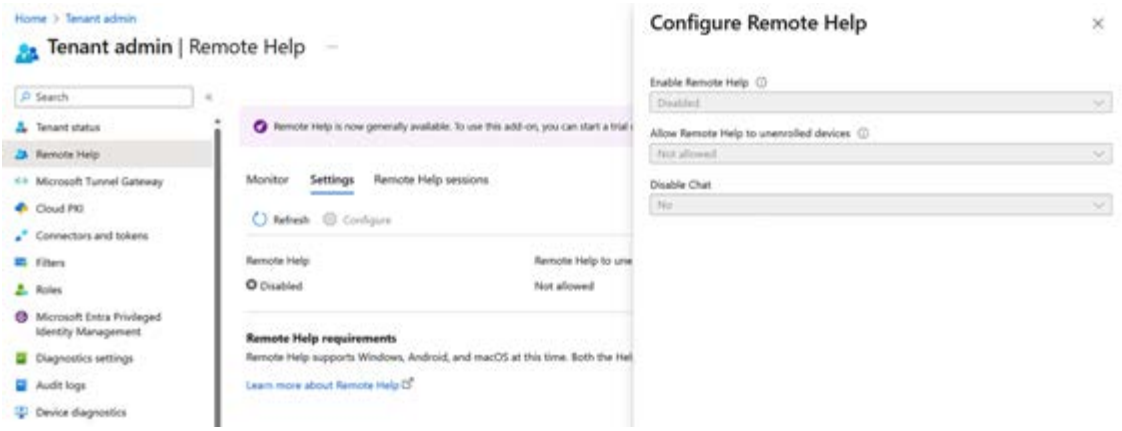


Figure 11.136: Configure Remote Help settings grayed out

This concludes the Remote Help section. Next up is the section on Advanced Endpoint Analytics.

Advanced Endpoint Analytics

Microsoft Intune Advanced Endpoint Analytics is a set of analytics-driven capabilities that helps IT admins understand, anticipate, and improve the end user experience.

The key capabilities of Advanced Endpoint Analytics are:

- Identify anomalies based on patterns of unexpected events and signals aggregated across enrolled devices.
- Discover meaningful patterns and trends by correlating anomalies to device configurations and properties like OS version and app/driver versions.
- Use an enhanced device timeline view that includes anomalies to ease and speed troubleshooting.
- Get detailed reports of the analytics, insights, and recommendations for a subset of devices using IT-defined scope tags.

If you have already enabled Advanced Endpoint analytics in your Microsoft Intune tenant, you can read more about this in *Chapter 14*, *Monitoring and Advanced Endpoint Analytics*. Once you have the Intune Suite license in your tenant, Advanced Endpoint Analytics features will show up without you, as an IT administrator, needing to do any kind of configuration.

To access Advanced Endpoint Analytics in Intune, follow these steps:

1. In the Microsoft Intune admin center, go to **Home** | **Reports** | **Endpoint analytics**.
2. Click on **Anomalies**.

   You will see **Device scope**, where you can change the report view based on the device scope.

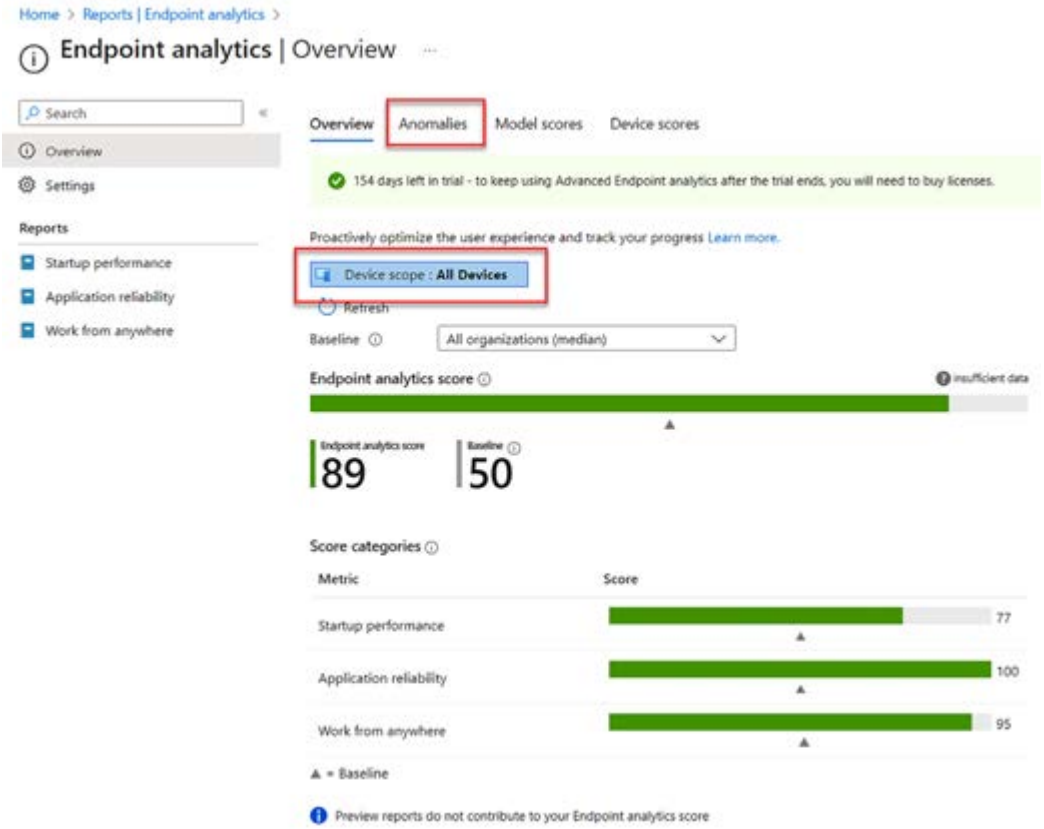


Figure 11.137: Endpoint analytics Anomalies

You can also access the Anomalies report in your tenant where you can filter by severity. The analytical model detects device cohorts facing an anomalous set of stop errors/restarts and application hangs/crashes that need admin attention to mitigate and resolve. Device cohorts are only identified for medium- and high-severity anomalies.

You can leverage this report to get information on anomalies across all your devices to help you proactively troubleshoot issues and root causes with your Windows estate.

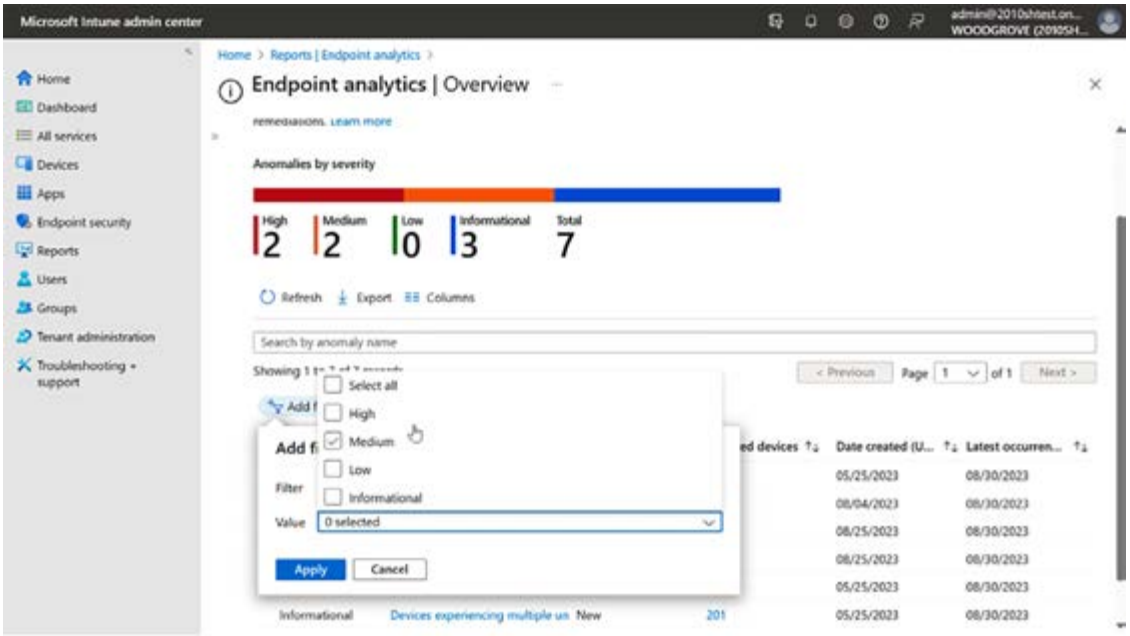


Figure 11.138: Endpoint analytics Anomalies report

To configure custom device scopes, you just need to click on **Manage device scopes**.

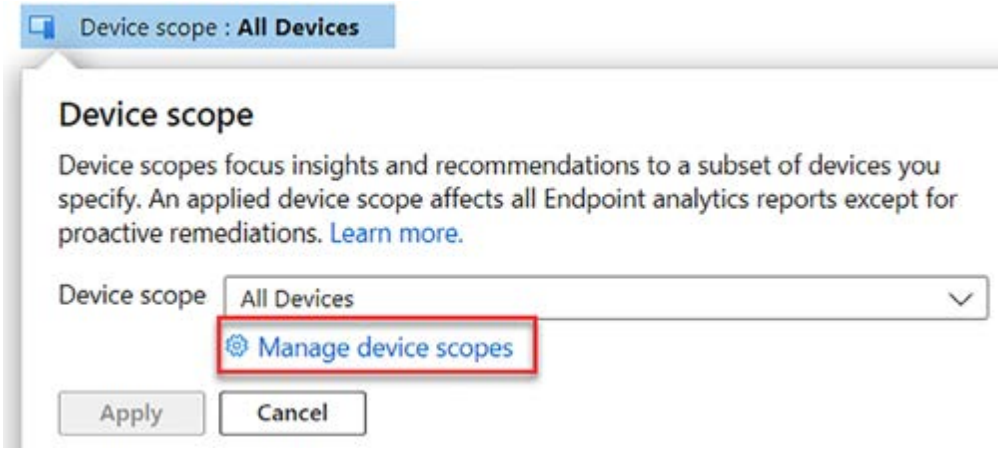


Figure 11.139: Managed device scopes

Then you can create new device scopes based on the scope tag. In this example, we have created a device scope for all Windows Autopilot devices as we have a specific scope tag for those devices. Another example is you can use a scope tag to segregate your devices based on countries.

There is a limit of 20 custom device scopes for Advanced Endpoint Analytics.

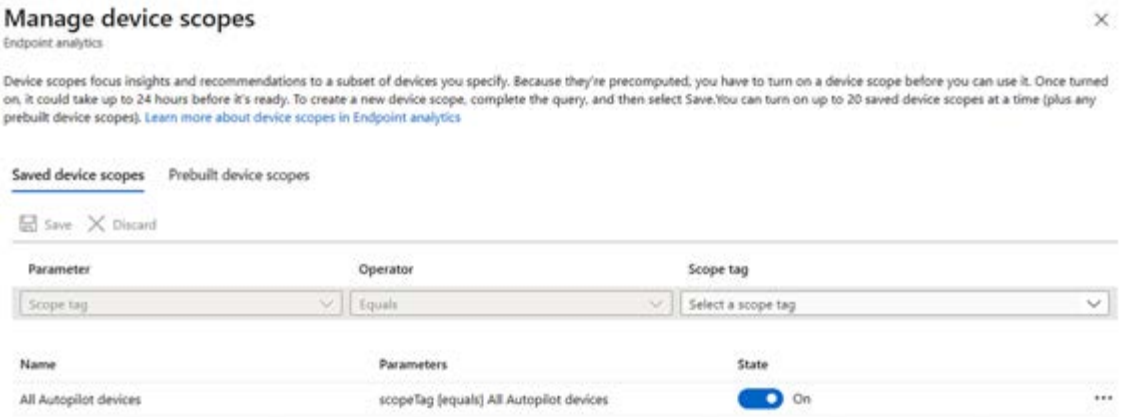


Figure 11.140: Saved device scopes

You can also look at the device timeline from a device perspective, by selecting the device in the Intune admin center. Click on **User experience | Device timeline**; this will give you detailed information about what happened on that device and when.

The **Device timeline** tab replaces the **Application reliability** tab in your tenant if you have advanced Endpoint analytics active.

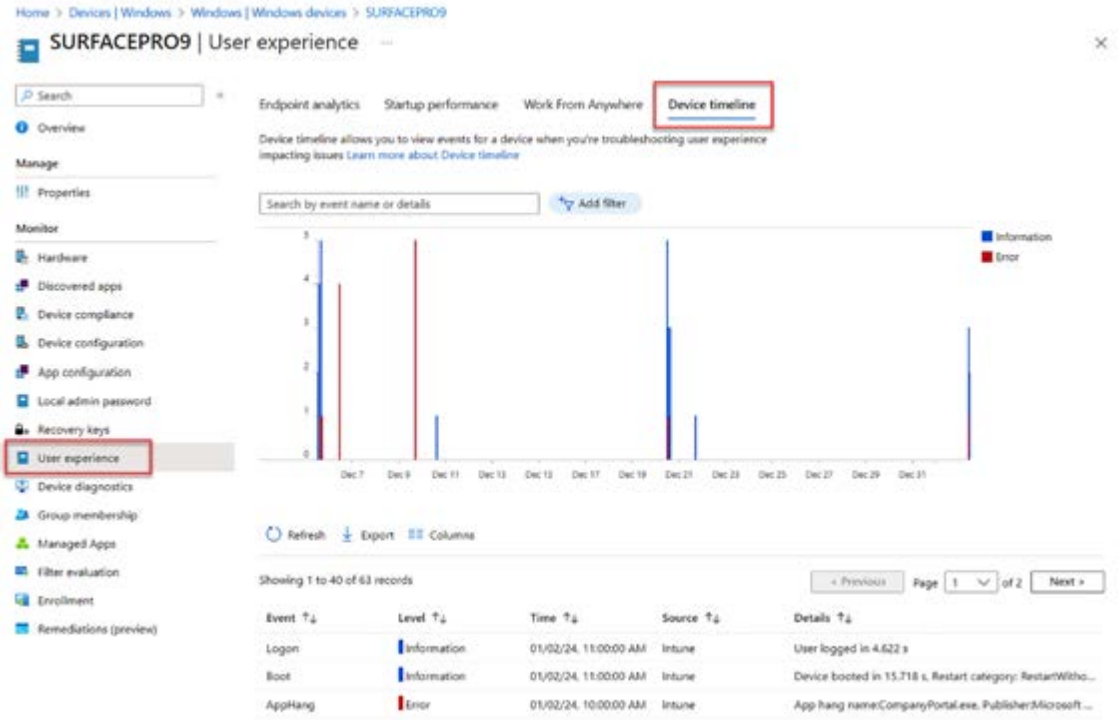


Figure 11.141: Device timeline

You can add filters for sources (like Intune or Intune anomaly detection) or for levels (like **Error** or **Critical**) before you search or you can just have an overview of the device timeline.

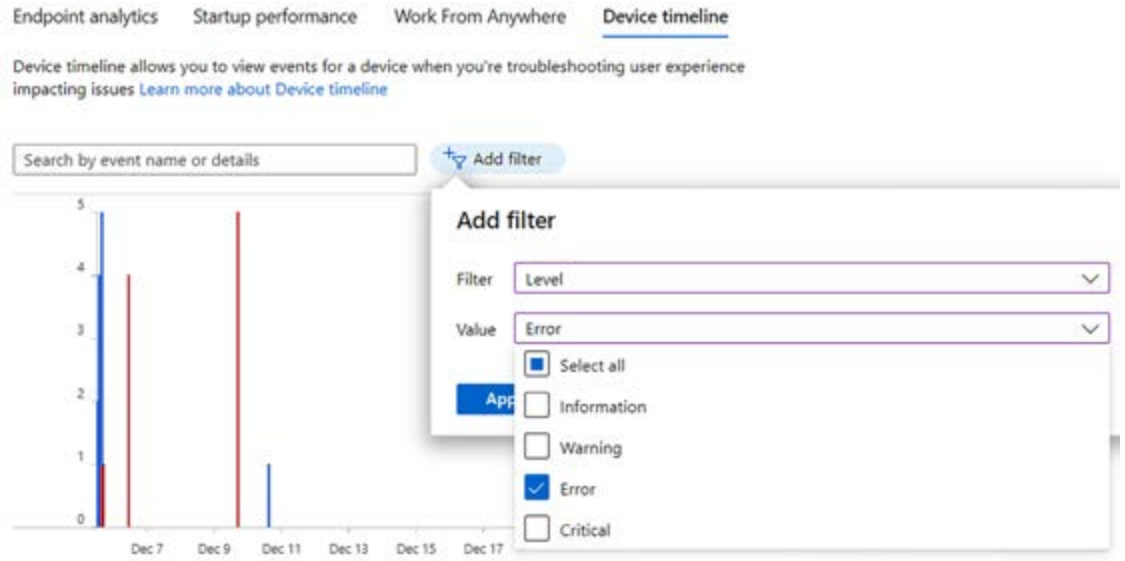


Figure 11.142: Device timeline – Error filter

Device query

For Windows devices that are natively cloud-managed, this feature offers an on-demand exploration of a device's operational information, spanning from hardware specifications, such as memory usage, to software configuration, including installed applications, registry keys, and networking settings. Think of this as an evolution of CMPivot, which required an on-premises Configuration Management infrastructure, whereas this can be used for all cloud-managed devices to gather real-time insights.

With Kusto queries on demand, you will be able to troubleshoot your device issues faster and more efficiently than ever before for all your Intune-managed devices.

You can only leverage **Device query** on Windows devices that are managed by Intune and are corporate-owned.

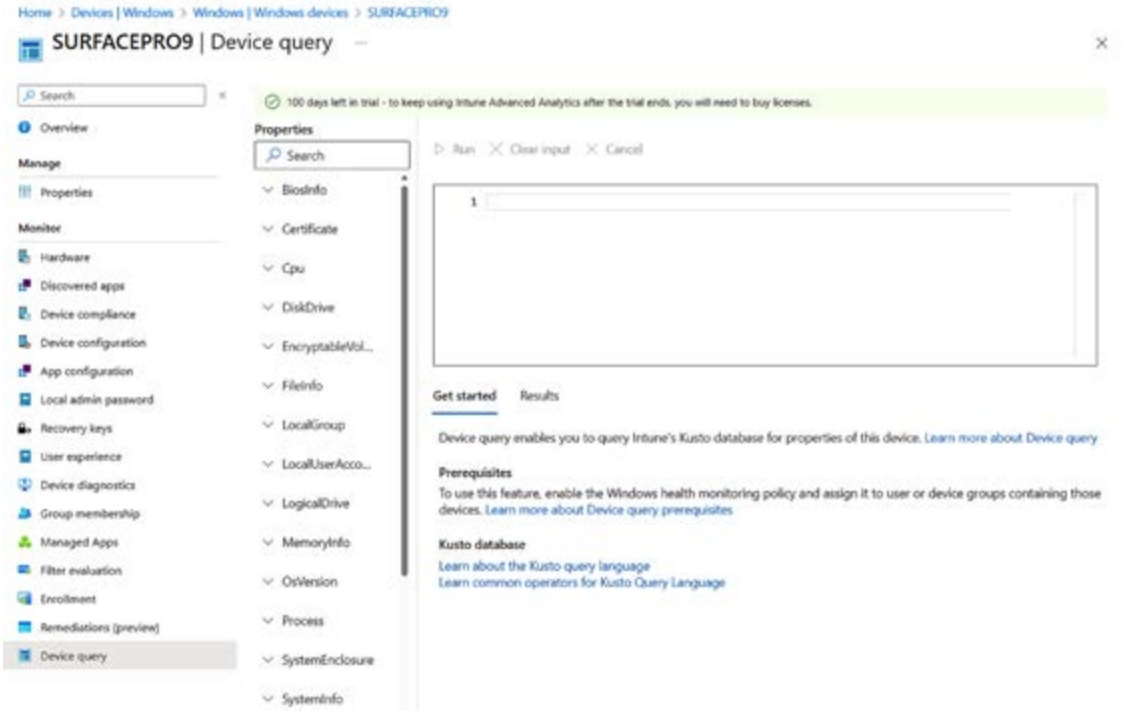


Figure 11.143: Device query

Let's look at a couple of good examples where you can benefit from **Device query**, as this information is not easily accessible from other places in Microsoft Intune.

In the first example, you can get a list of all local users on a device by running this **Kusto Query Language (KQL)**:

```
LocalUserAccount
| where c
```

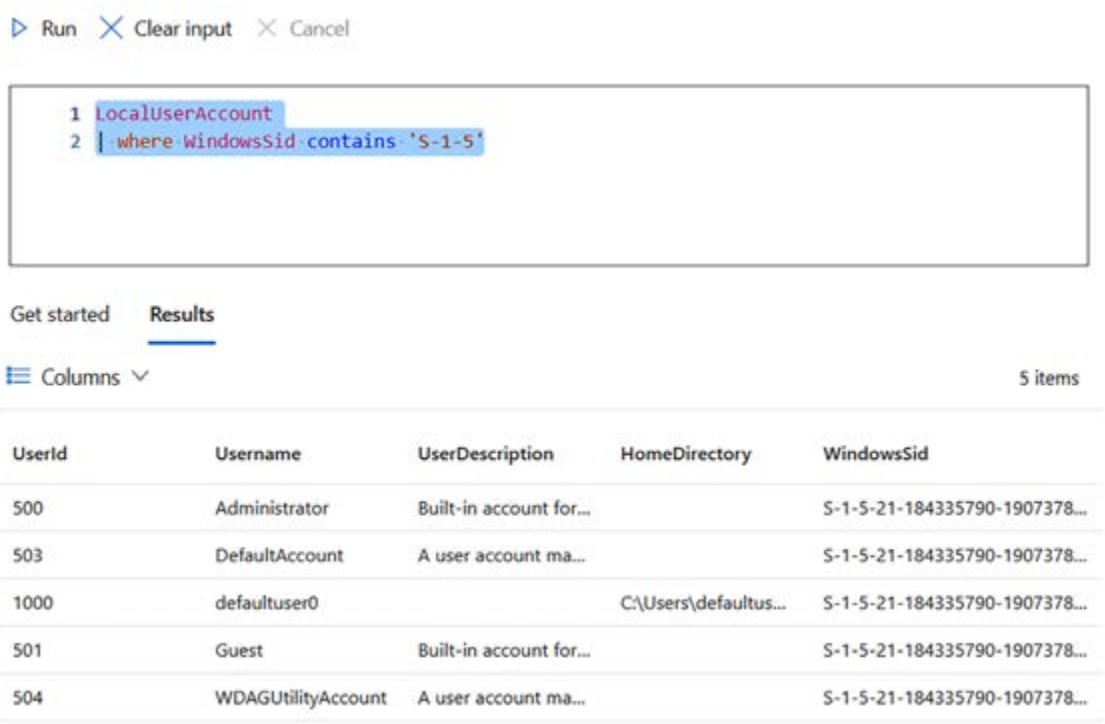


Figure 11.144: Device query LocalUserAccount

In the second example, you can get a list of your drive's BitLocker encryption status, including the encryption method, which is not available in any report in Intune:

```
EncryptableVolume
| join Tpm
| project WindowsDriveLetter, ProtectionStatus, EncryptionMethod,
EncryptionPercentage, Activated, Enabled, SpecVersion, Manufacturer
```

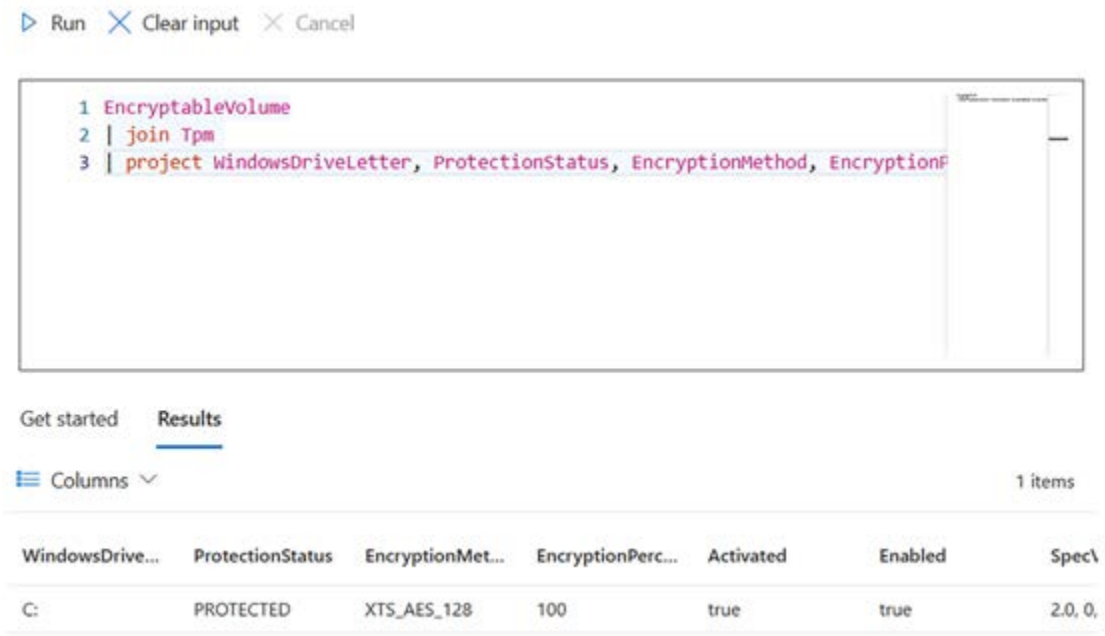


Figure 11.145: Device query BitLocker status

Battery health

With the Battery health feature inside Advanced Endpoint Analytics, it is the start of a new journey to support your organization with hardware insights so you can proactively address hardware issues that could be solved by replacing an unhealthy battery on your end users' laptops. This report provides IT admin with valuable insights on battery runtime, use cycles, charging capacity, and overall battery health information.

In the **Advanced Endpoint Analytics** blade, under **Battery health**, you get a complete view of your entire device estate's battery health. You can also explore these different views:

- **Device performance**: Performance per device, where you can see the max. and min. capacity.
- **Model performance**: Performance per hardware model (requires a minimum of 10 devices of the same model to show data).
- **OS performance**: Performance per OS version (requires a minimum of 10 devices on the same OS version).

- **App impact:** Where you can see what apps on your devices are consuming the battery and the percentage of the cumulative battery charge that the app consumed recorded.

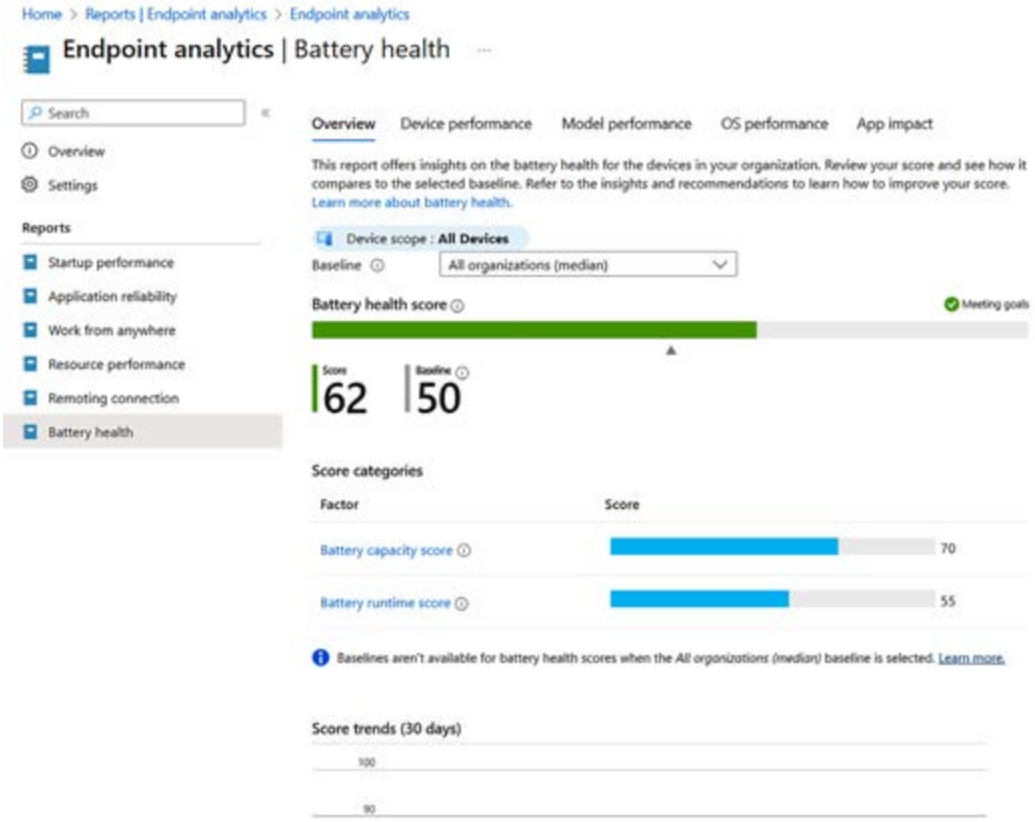


Figure 11.146: Battery health

You also have the option to view the battery health per device if you go to the **device | User experience | Battery health.**

This gives you a detailed view, including how many cycle counts the battery has and the maximum capacity.

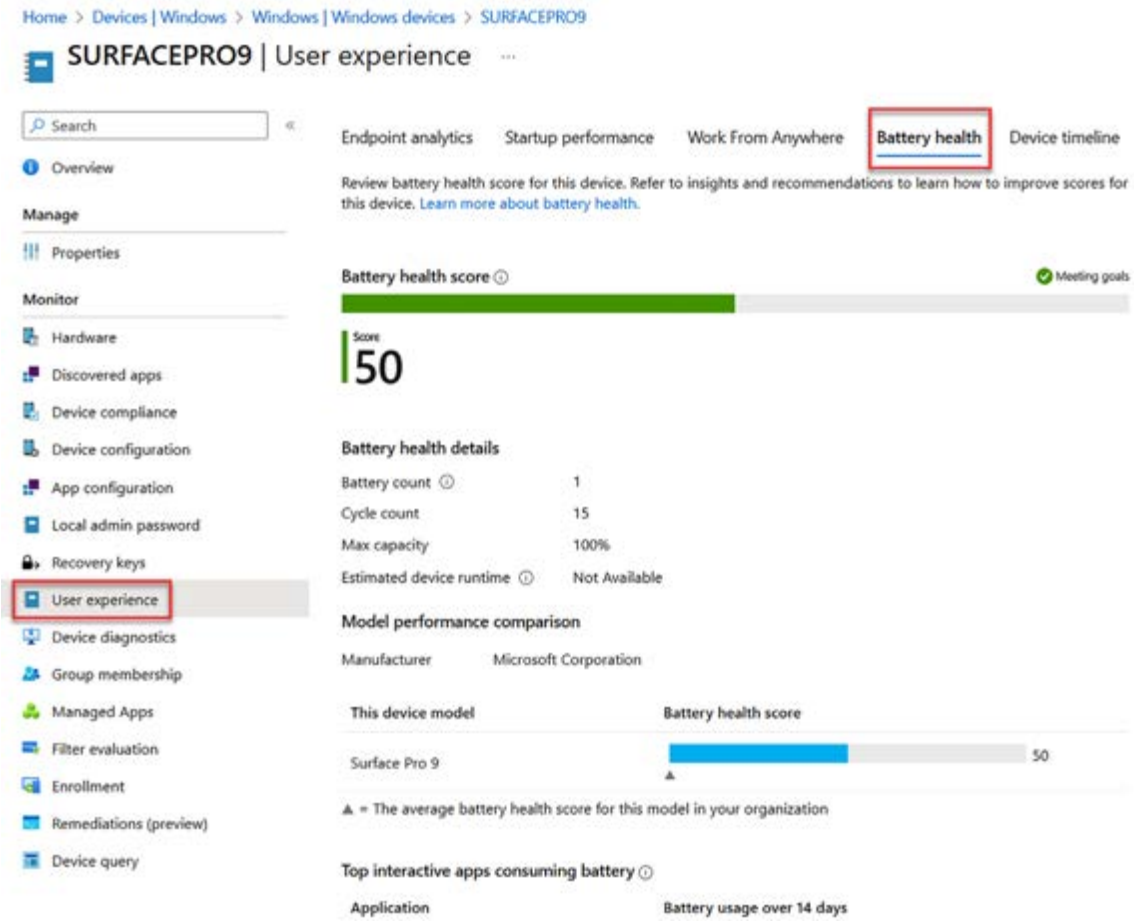


Figure 11.147: Battery health per device

This concludes the section on Advanced Endpoint Analytics. Next, we will discuss why Windows 365 and Intune are a great combination.

Why Windows 365 and Intune Suite are a great combination

It would be hard to name a better pairing than Windows 365 and Intune – at least that was the case before the launch of the new Microsoft Intune Suite.

Windows 365 empowers the security of your Cloud PCs but by combining it with Intune Suite components such as EPM to improve their security posture, drive efficiency for IT teams, and boost productivity, it really becomes zero-trust on steroids!

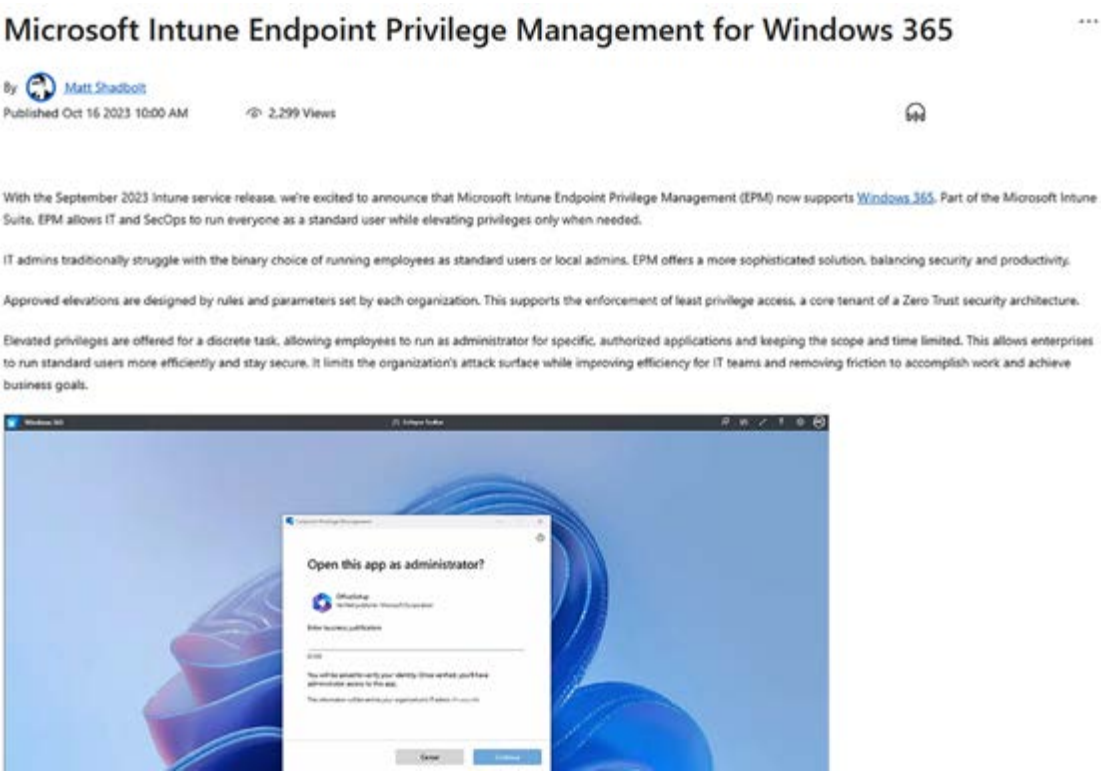


Figure 11.148: EPM on Windows 365

You are also able to remotely support your Windows 365 end users with Intune Remote Help, as you can scope your Windows 365 Advanced Endpoint Analytics reports with the built-in device scopes for Windows 365 Cloud PCs.

You can put the pedal on the metal even more with Enterprise App Management, as it leverages the familiar Intune Win32 app model to deploy third-party apps to your Windows 365 devices' estate!

Last but not least, you can modernize CA server infrastructure with Cloud PKI to deploy certificates to VPNs, for example, so you don't need an on-premises PKI infrastructure when you move your devices to the cloud with Windows 365.

Summary

This concludes the last of the chapters relating to Intune Suite. We've explained what Intune Suite is, how you can request a trial, and how to configure it as an IT admin and use it as an end user. Intune Suite will soon become one of the mainstream services used by enterprises. With this chapter, we wanted you to feel confident talking about both the business benefits as well as technical details – and we hope we succeeded!

In the next chapter, you will learn about the different tools that are available for profile management.

Questions

1. What license do you need for Enterprise App Management?
    a. Intune Core
    b. Intune Suite
    c. Windows E3 or E5
2. Does EPM support IT admin approval for the elevation of installation rights?
    a. Yes
    b. No
3. Windows 365 Cloud PCs and EPM take zero-trust and security to the next level!
    a. True
    b. False

Answers

1. (b)
2. (a)
3. (a)

Further reading

If you want to learn more after reading this chapter, please use the following free online resource:

- *Overview Intune Suite*: `https://learn.microsoft.com/en-us/mem/intune/fundamentals/intune-add-ons`

Get This Book's PDF Version and Exclusive Extras

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

Note: *Keep your invoice handy. Purchases made directly from Packt don't require one.*

UNLOCK NOW



12

Copilot/AI

In this chapter, you'll learn about Microsoft's latest generative AI functionalities for both Windows and Microsoft Intune via the Windows and Security Copilot integrations. Some of the material is still in early preview – however, we didn't want to omit it from this book as AI will fundamentally change the way we manage and use our computers in the future (if it hasn't done so already!). Some of the features might already be available when you're reading this book!

In this chapter, we will be taking a deep dive into Security Copilot and introduce a wide range of products embedded integrations; we will focus on the upcoming Intune integrations for device management but also highlight some other new use cases.

Let's start this chapter!

In this chapter, we will cover the following topics:

- The future of AI in Windows and Intune
- Copilot in Windows
- What can you use Copilot in Windows for?
- Security Copilot (device management)
- Intune policy validation via Security Copilot
- Troubleshooting Intune via Security Copilot

The future of AI in Windows and Intune

The year of the AI PC: that's what we both believe this year and upcoming years will be. Copilot is an extremely powerful generative AI tool based on **Generative Pre-trained Transformers** (**GPTs**) that Microsoft created for product integrations in Windows (Windows Copilot) and Microsoft Intune (**Security Copilot**). GPTs are created by OpenAI.

With Copilot, you can customize your experience to fit your needs, whether you're an IT admin or an individual user. Copilot is powered by AI, making it easier to stay on top of your security and manage your devices. With Windows and **Security Copilot**, you can have peace of mind, knowing that your devices are always protected.

With Windows 365, you will be able to use **Copilot in Windows** from any device, anywhere, and from any platform! Copilot is also available via your browser at `copilot.microsoft.com`.

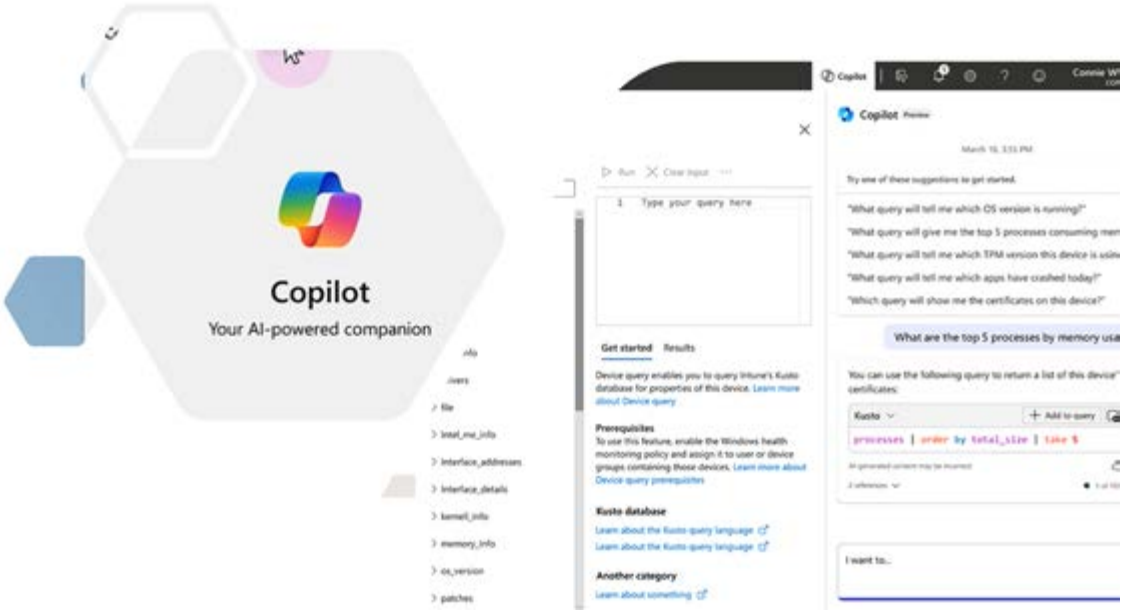


Figure 12.1: Copilot, your AI-powered companion

Copilot in Windows

In *Chapter 1*, we briefly talked about Copilot in Windows and how it can help you navigate Windows via AI. Copilot in Windows is integrated with Microsoft Copilot, which makes it easy to search for internet results directly without opening Bing.com!

To use Windows Copilot, click on the new Copilot button located on the taskbar to activate Copilot in Windows, or use the shortcut *Windows + C* to jump right in! Copilot in Windows links to Microsoft Copilot using the same Microsoft account or Microsoft Entra account that you used to log in to Windows.

New laptops will also include a Copilot button on the keyboard!



Figure 12.2: Windows 11 Start menu with Copilot

When you click on the **Copilot** button, the Copilot navigation panel will show up on the right side of the Windows desktop screen.

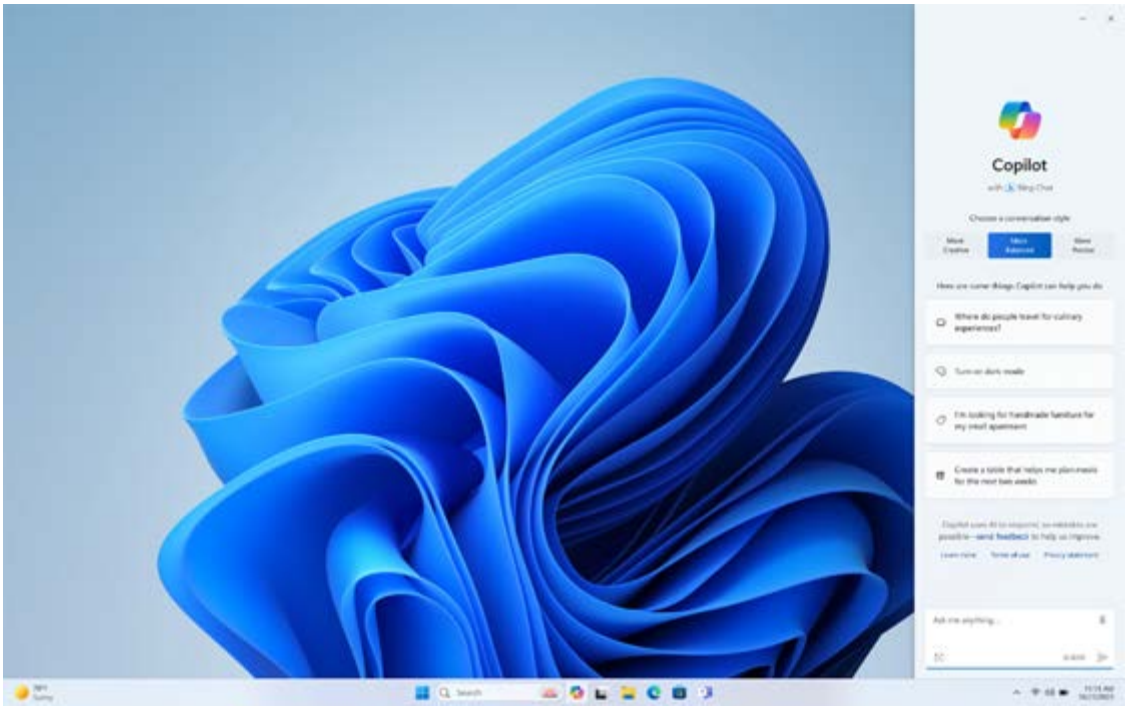


Figure 12.3: Windows Copilot navigation panel

What can you use Windows Copilot for?

Copilot in Windows can answer a variety of questions, from the simplest to the most complex. For instance, if you're considering a trip to Cyprus during the mid-winter break, Copilot in Windows can assist you in finding flights and accommodation. As you type in the chat pane, Microsoft Copilot offers autocomplete suggestions to simplify your chat experience.

Copilot in Windows can leverage context from Microsoft Edge to enrich its responses. It allows you to request a summary of a webpage you're currently viewing, without the need to provide the website address or copy and paste extensive text. Copilot in Windows is integrated with the clipboard and supports drag-and-drop for images, facilitating rich interactions and enabling you to accomplish tasks more quickly.

Copilot in Windows offers three distinct chat tones. You can switch the chat tone from **Precise**, which provides shorter, search-focused answers, to **Creative**, which delivers longer and more descriptive responses. The **Balanced** setting offers a middle ground between the two. **Light** and **Dark** modes are also supported.



Figure 12.4: Windows Copilot dark mode

Copilot in Windows also allows you to change Windows settings you normally configure manually in the **Settings** menu.

For example, you can switch your Windows theme from light to dark mode, or you can activate the **Do not Disturb** feature if you are engrossed in work and want some privacy, or you can also connect Bluetooth devices seamlessly. It even allows you to launch applications such as Office, or arrange your application windows, among all the other functions.

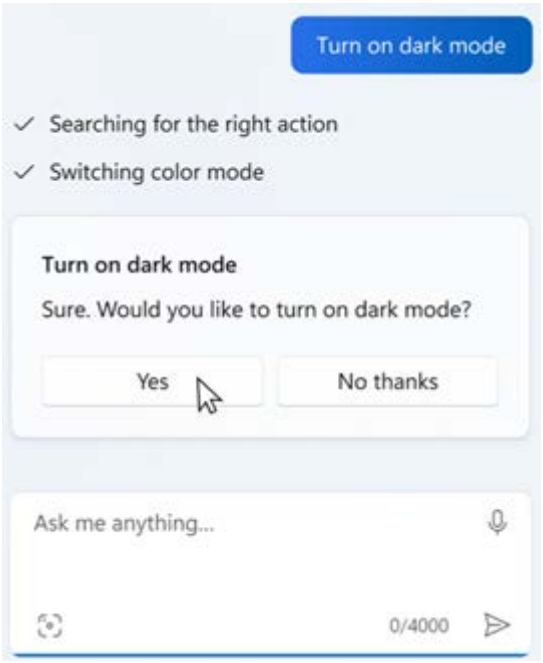


Figure 12.5: Windows Copilot

Here are some chat examples you can use Copilot in Windows.

Direct instructions

- Turn on dark mode
- Mute volume
- Change wallpaper
- Take a screenshot

Questions

- Why isn't my audio working?



In the latest Windows 11 builds, Windows Copilot now launches in an expanded window to give you more space to chat. You can resize it and easily switch back to a thinner side-by-side window too!

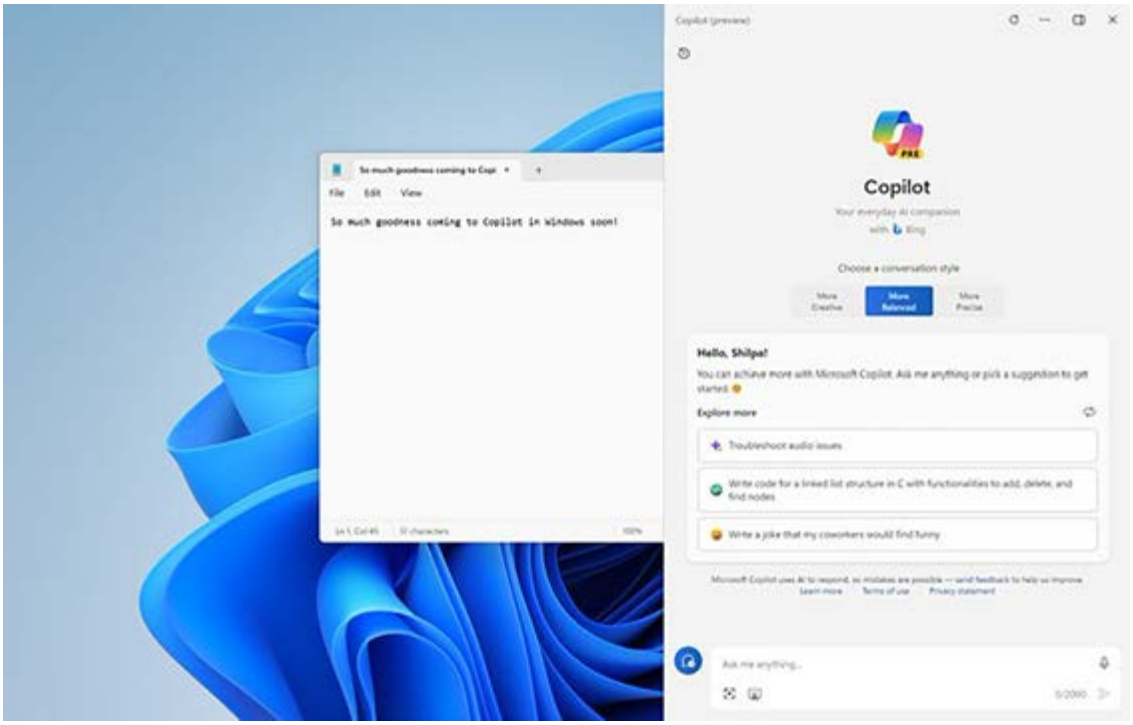


Figure 12.6: Windows Copilot xpanded window

Follow these steps to create a custom profile to control Copilot in Windows with a template in Microsoft Intune – Copilot in Windows uses the new CSP WindowsAI, which currently only has one policy setting to simply turn Copilot off.

This is a user policy only and requires a specific Windows version to be applicable:

- Windows 10, version 22H2 Build 10.0.19045.3758 and later
- Windows 11, version 22H2 Build 10.0.22621.2361 and later
- Windows 11, version 23H2 Build 10.0.22631 and later

Are you an IT administrator who wants to turn off Copilot for your end users? Copilot in Windows is enabled by default on Windows 10 and Windows 11 (latest builds). While we hope you are going to leverage this beautiful piece of innovation, but we also understand that you might want to disable it. Here are the steps to perform to achieve this:

1. For **Profile type**, select **Templates.** For **Template name**, select **Custom.** Then, click **Add:**

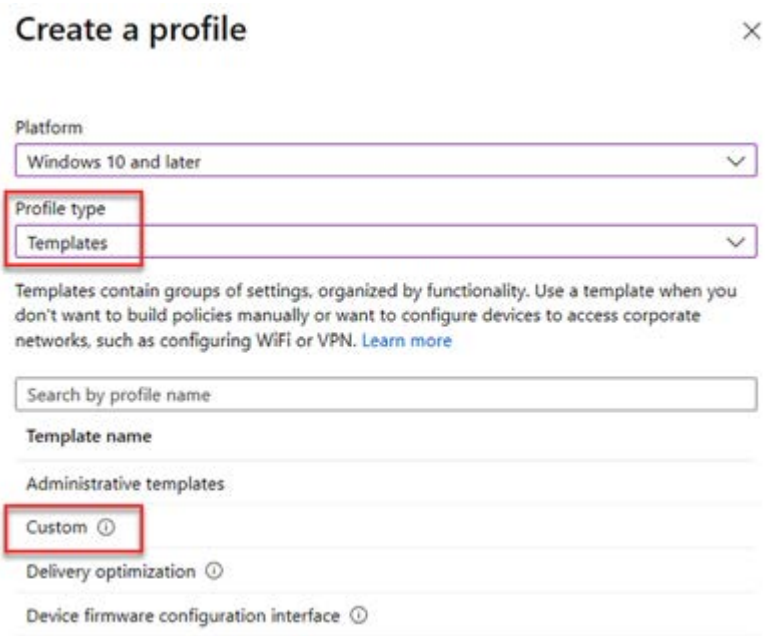


Figure 12.7: Templates – Custom

2. By clicking **Add**, you can fill out all the required values in the **Add row** blade. You can add as many rows as you need to the policy you are creating:

    - **Name: Disable Windows Copilot.**
    - **OMA-URI:** Enter the following path, which is case-sensitive, and avoid trailing spaces: `./User/Vendor/MSFT/Policy/Config/WindowsAI/TurnOffWindowsCopilot`.
    - **Data type:** Select **Integer**.
    - **Value:** `1`.

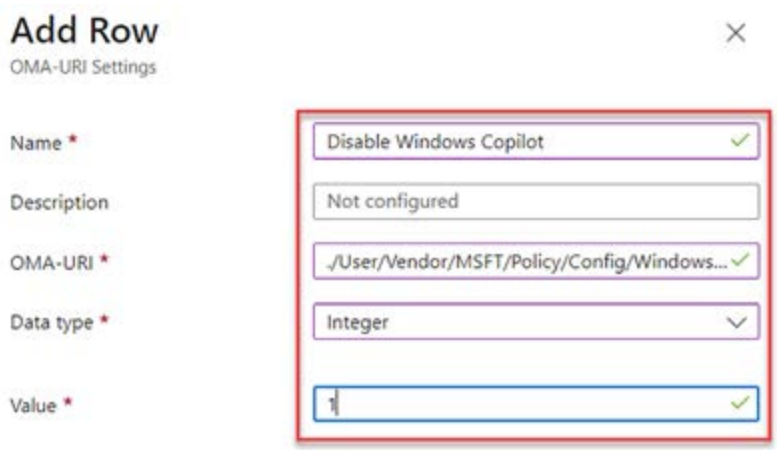


Figure 12.8: OMA-URI settings

Security Copilot (Device Management)

Security Copilot is a new OpenAI GPT-based tool offered as a cloud-based service to bolster the security of your Microsoft security cloud services, of which Microsoft Intune is a part. Microsoft Security Copilot addresses this query and illustrates how to utilize this innovative AI tool. It employs real-world examples to delve into how Security Copilot aims to disrupt conventional methods across diverse cyber security domains.

As mentioned in the previous section, Security Copilot is built for all Microsoft security services, including Security Operations, Device Management, Identity Management, Data Protection, Compliance, and Cloud Security. For this chapter, we will be focused on using Security Copilot and **Device Management** as a device assistant, as an error analyzer, to compare devices, and to simplify the creation of advanced queries for Microsoft Intune.

So, let's explore together what Security Copilot can do to help you as an IT administrator/organization to streamline your Intune processes!



The following images represent work-in-progress features of Intune. Feature capabilities, designs, and visual elements are subject to change for final release.

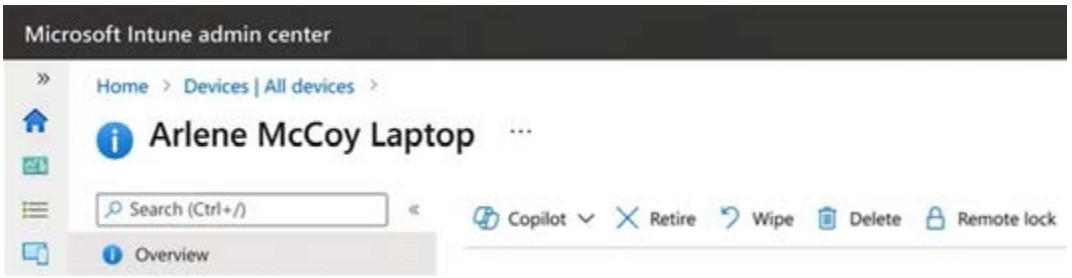


Figure 12.9: Intune features

Intune policy generation via Security Copilot

One of the most important elements of configuring Microsoft Intune for Windows devices, whether for physical or cloud PCs, is assigning policies to make the device secure and tailored to your company's preferences. How cool would it be to make it much easier to test the assignment of your policies with Security Copilot? Well, let's show you how this works...

In this example, we will use Security Copilot to summarize new policy configurations for validation and review. As you can see, in this example, we're assigning a new BitLocker policy to our Windows 11 devices:

1. You will see a new **Summarize policy** option. Let's click on it.

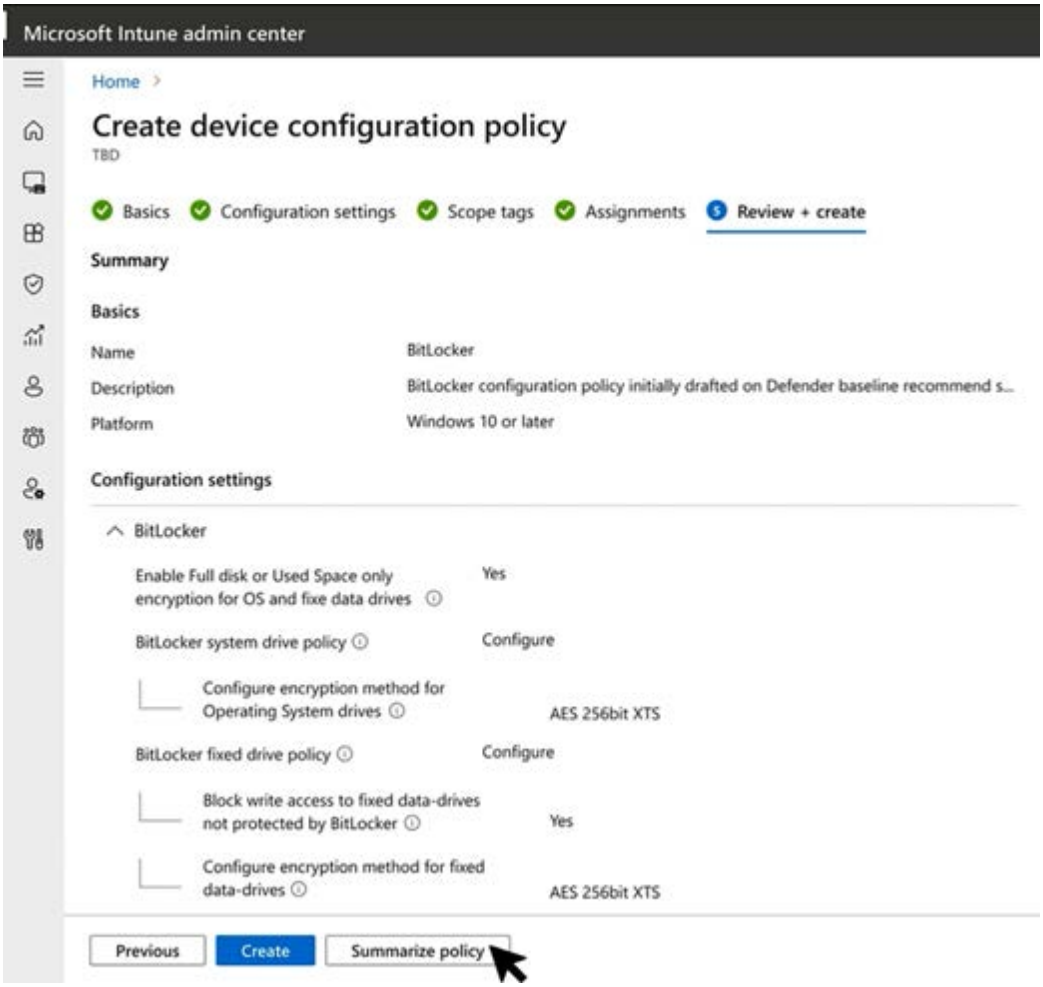


Figure 12.10: Intune Copilot

2. The Security Copilot navigation pane opens in the bottom-right corner of the Microsoft Intune admin portal. As part of the process, Security Copilot will now provide a summary of the policy. We can easily share this information with our co-workers in the IT department, but it also gives us insights as to whether the policy actually does what we want before creating the policy.

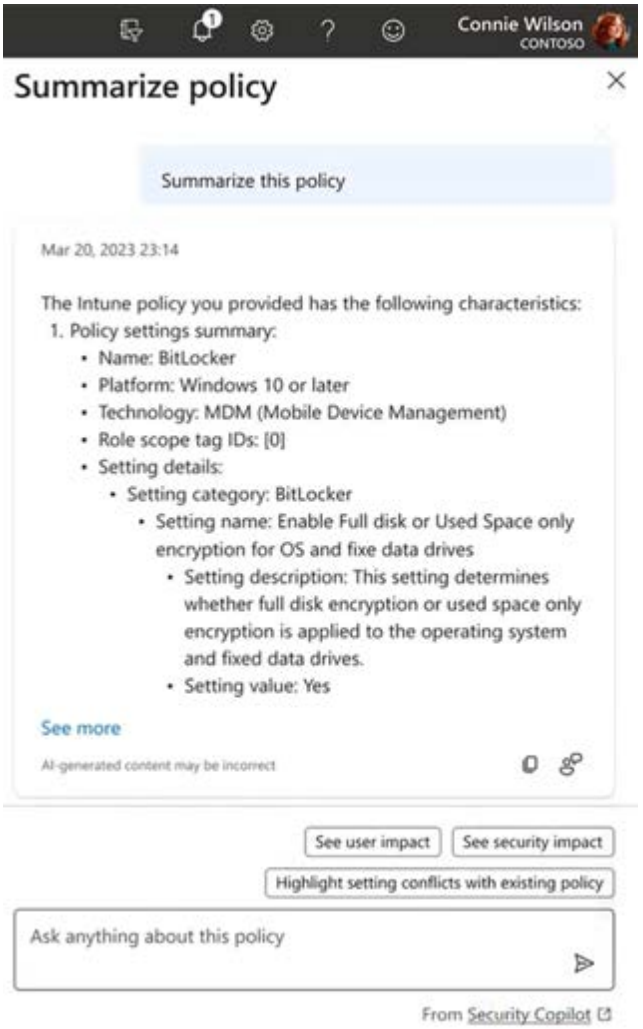


Figure 12.11: Intune Copilot

3. Now the real *power of Copilot kicks in*, as Copilot can give you real-time insights as to what settings do before applying them. This is called the **setting assistant feature.**

4. Here we are in another device configuration policy. We want to be sure that the policy applies in the right way and doesn't conflict with any other configured settings.

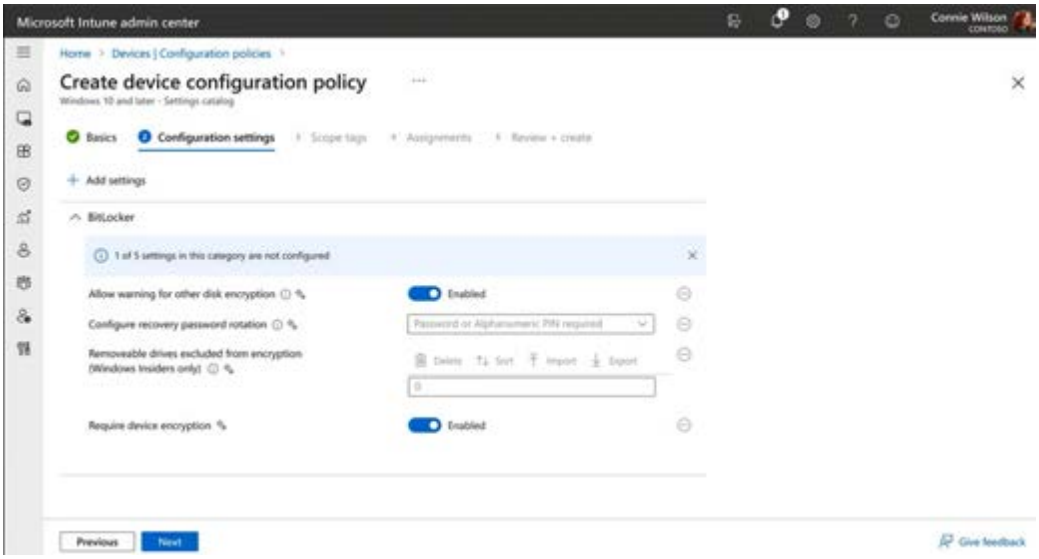


Figure 12.12: Intune Copilot

5. You can open the Security Copilot setting assistant feature via the **two stars** icon next to the information button, as shown below.

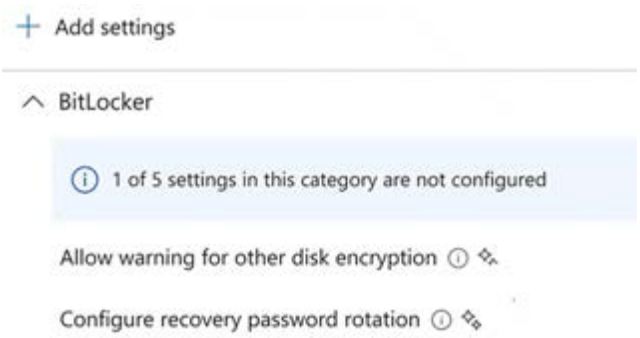


figure 12.13: Intune Copilot

6. Once the Security Copilot navigation pane opens, it will automatically ask about the **Allow warning for other disk encryption** setting and provide you with insights about what the setting applies.

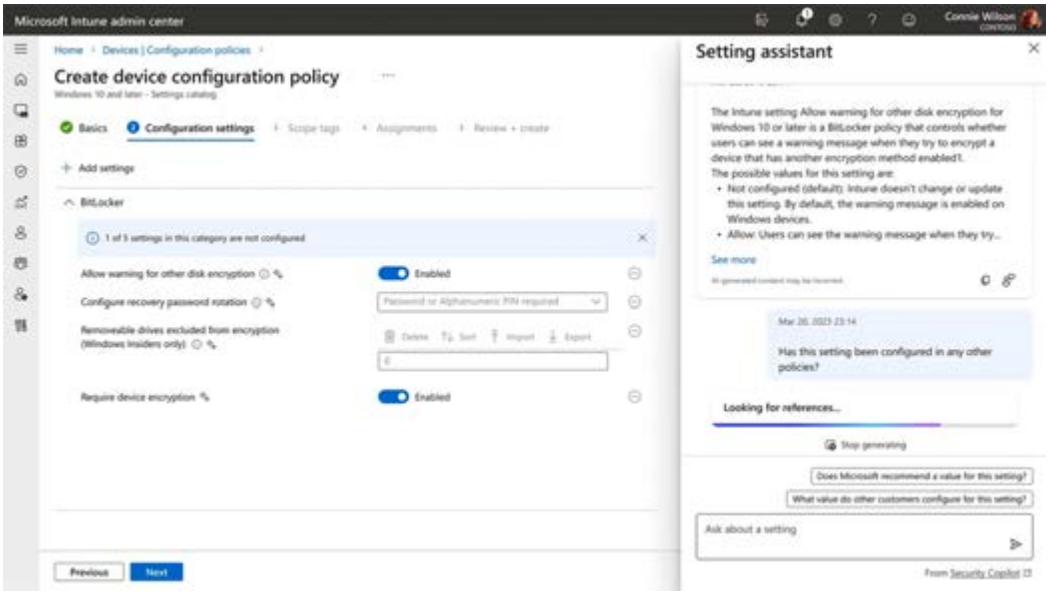


Figure 12.14: Intune Copilot

7. This told us everything we needed to know about the setting without searching the documentation or leaving the workflow.

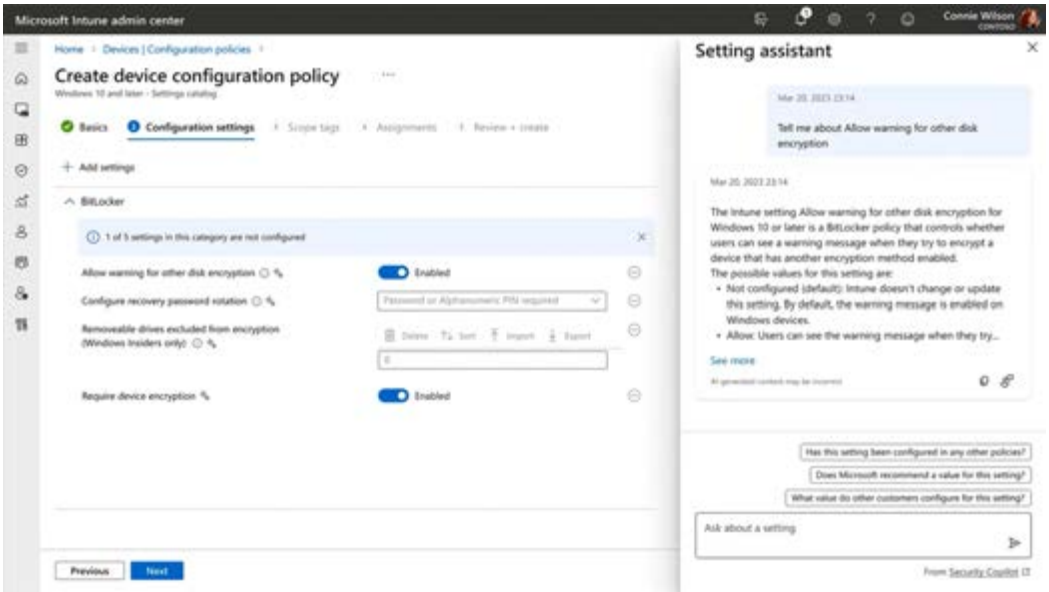


Figure 12.15: Intune Copilot

8. What if we want to go one step further and ask Security Copilot whether this setting has been configured already to avoid duplication or any other errors?

   Let's click on the suggested question: Has this setting been configured in any other policies?

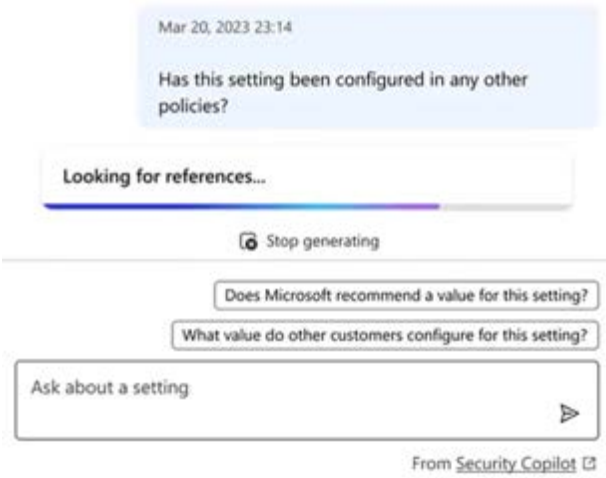


Figure 12.16: Intune Copilot

9. You can see that the setting has been configured already somewhere else. We can now choose to disable this policy from the Copilot menu directly or work with our co-workers to align on the right policy structure moving forward. All in a single click – very convenient!

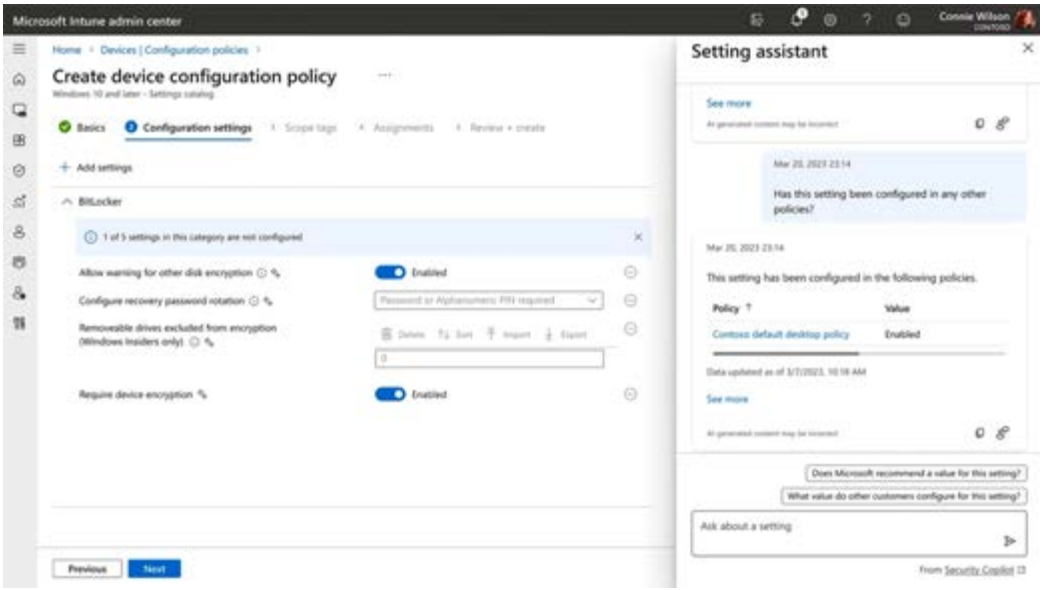


Figure 12.17: Intune Copilot

Copilot assistant for Intune device queries

Experience the power of Copilot with the device assistant, designed to provide effortless insights into your device's key aspects. Whether you need help with troubleshooting, understanding configuration details, or any other inquiries, this dynamic duo ensures a swift and precise response, thereby enhancing your device management experience.

Getting help is easier than ever with the introduction of the new **Copilot** button in the actions menu. To start resolving any device issues, all you need to do is click the **Copilot** button.

This user-friendly feature streamlines the process, making it simpler than ever to harness the power of Copilot for efficient problem-solving and device support. With just a single click, you can unlock a world of assistance tailored to your device needs. Explore this simplicity today!

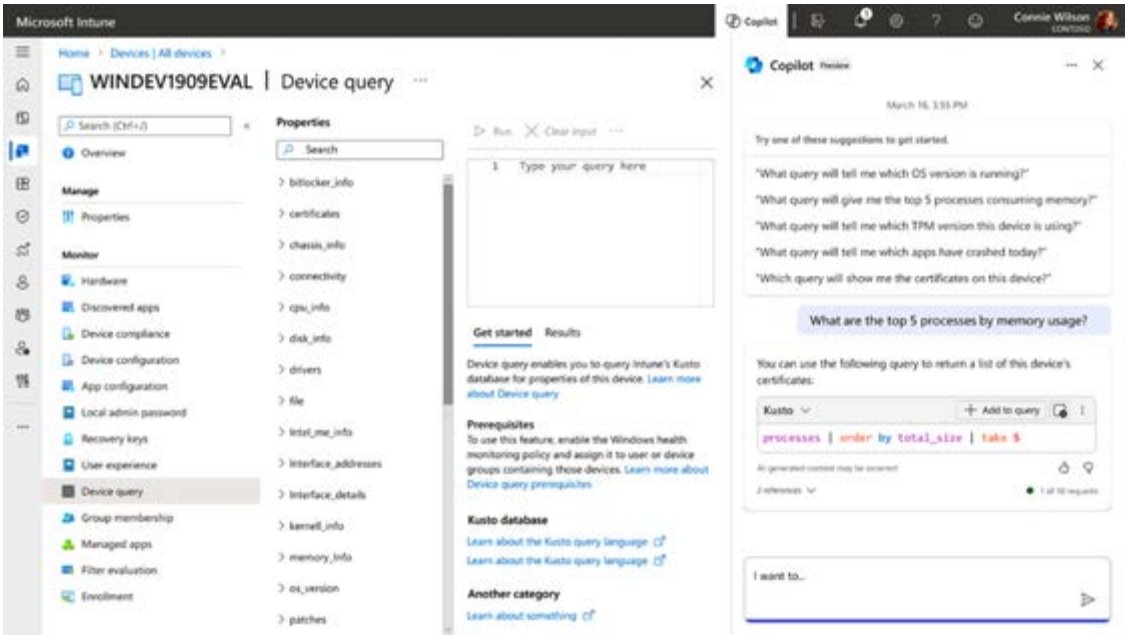


Figure 12.18: Intune Copilot

In the next section, we will look at troubleshooting Intune Copilot.

Troubleshooting Intune via Security Copilot

In this section, we will be giving you a sneak peek into how Security Copilot helps you with device troubleshooting in Microsoft Intune. Below, you see Arlene's Windows laptop, which has slow startup issues reported by the user.

An IT admin can use Copilot to gather all information, from various sources, about the device that could help with analysis of the current state of the device or fleet of devices.

Troubleshooting

1. Find and understand everything you need to know about the given device.
2. Analyze the Intune error codes (Apps, Policy, Updates, Scripts, Enrollments).
3. Compare the settings on two devices to understand potential misconfigurations.

The IT admin or service desk user should go to **Devices | All devices** to start troubleshooting the issue via Copilot.

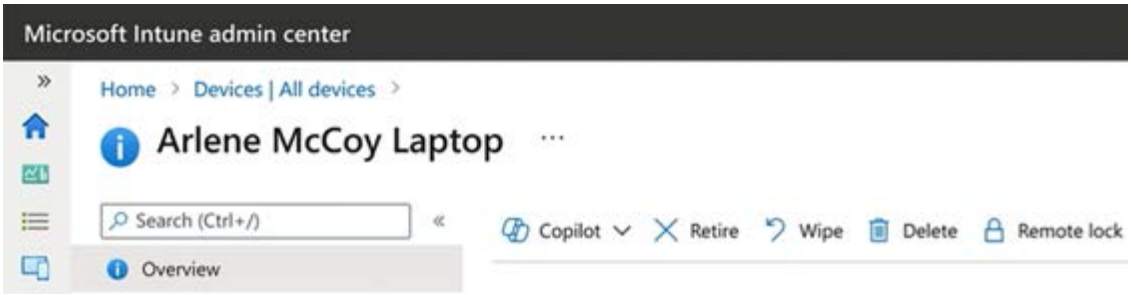


Figure 12.19: Intune Copilot

When you click on the **Copilot** button, the dropdown will give you a couple of options to pursue. We will go for the third option:

1. Explore device
2. Compare device
3. Ask about errors

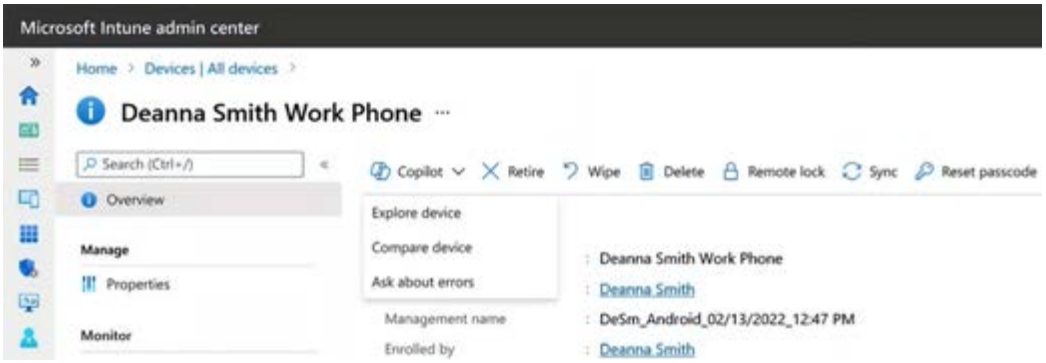


Figure 12.20: Intune Copilot

4. The user's device has a slow startup time, as you can see. The device has been restarted, but that didn't fix the issue. Let's ask Security Copilot what the issue might be...

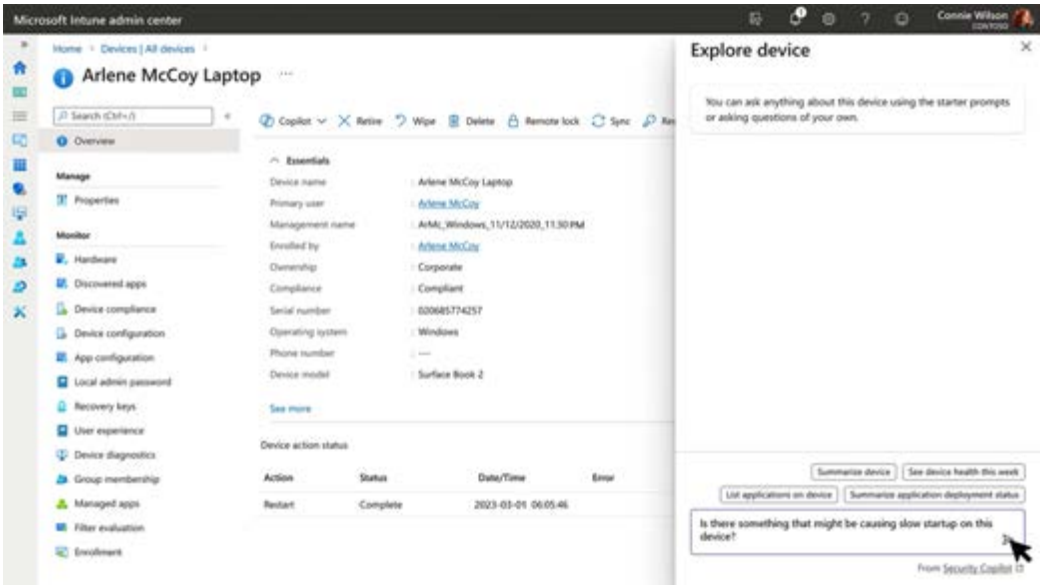


Figure 12.21: Intune Copilot

5. Copilot explores the device logs and concludes that the startup process is influenced by the VPN software. We hear you thinking, it's always about... (the network).

   This is just one great example of how you can easily troubleshoot Windows or other endpoint devices via Security Copilot in Microsoft Intune!

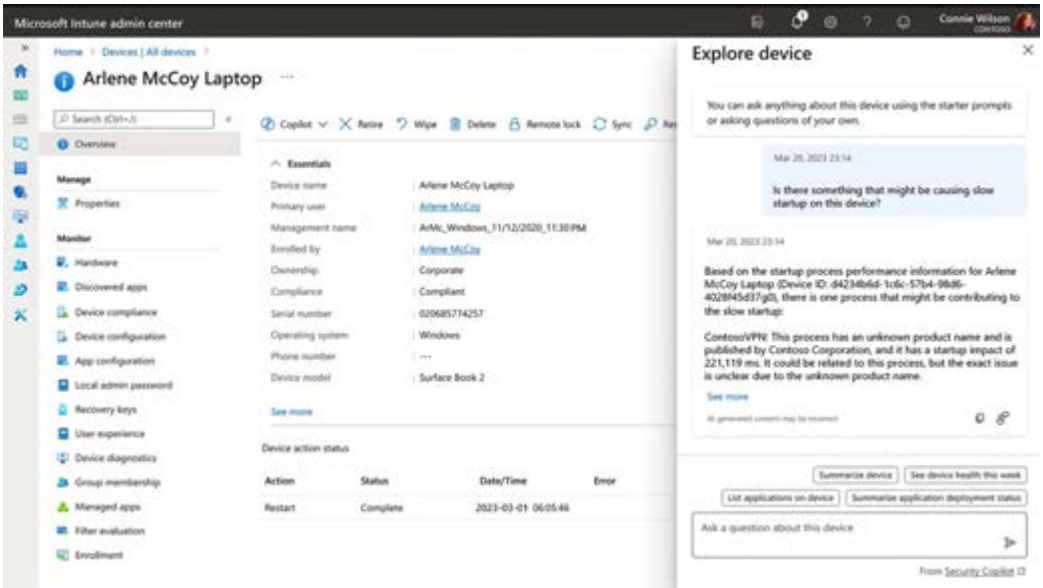


Figure 12.22: Intune Copilot

6. If there a specific resolution, Security Copilot will try to resolve the issue or point you to Microsoft documentation to read about how to solve it as an IT administrator. The last resort would be creating a Microsoft support ticket.
7. There are also specific other follow-up actions that Security Copilot provides as suggestions above the text field, such as **See device health this week**. This can be very handy to navigate your way through the resolution more proactively!

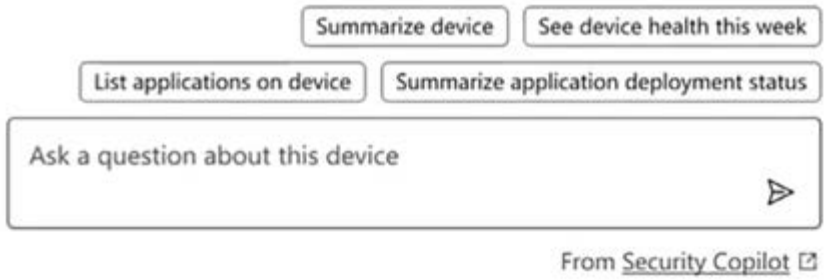


Figure 12.23: Intune Copilot

Summary

This concludes our chapter on Copilot, the new powerful tool that provides new integrations via Microsoft's industry-leading generative AI technology. Hopefully, you learned how the different versions of Copilot help you as an IT admin to simplify management and deployment for Microsoft Intune and other cloud services.

In the next chapter, you will learn about the different tools that are available for profile management.

Questions

1. What Copilot version does Microsoft Intune integrate with?
    a. Azure Copilot
    b. Security Copilot
    c. Windows Copilot
2. Can you configure Intune policies via Copilot?
    a. Yes
    b. No

Answers

1. b
2. a

Further reading

If you want to learn more after reading this chapter, please use the following free online resources:

- *Overview of Security Copilot*: `https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot`
- *Security Copilot customer scenarios*: `https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot?rtc=1#customerstories`

Join the CloudPro Newsletter with 44000+ Subscribers

Want to know what's happening in cloud computing, DevOps, IT administration, networking, and more? Scan the QR code to subscribe to **CloudPro**, our weekly newsletter for 44,000+ tech professionals who want to stay informed and ahead of the curve.

`https://packt.link/cloudpro`

13

Identity and Security Management

In this chapter, you will learn everything about **Entra ID join** and security. We will cover the history of Entra ID and the different security aspects that you can configure to secure your Windows 10 or Windows 11 Enterprise devices within your organization.

In this chapter, we'll go through the following topics:

- Microsoft Identity
- Entra ID
- Users and groups
- Entra ID join or Hybrid Entra ID – What's the best option?
- Conditional Access
- BitLocker disk encryption
- Personal Data Encryption
- Self-service Password Reset
- Entra ID password protection
- Passwordless authentication
- What is and isn't supported in each passwordless scenario
- Application Control for Business
- Windows Local Administrator Password Solution
- Microsoft Defender for Endpoint
- Screen capture protection and watermarking

Microsoft Identity

Active Directory Domain Services (**AD DS**) has been on the market since the year 2000. As you might remember, it arrived with the first release of Windows 2000 Server.

The way it works is, you join your Windows client or server devices to **Active Directory** (**AD**) to take over its management layer via either group policies or security settings, or you use it to chain different AD environments to each other to delegate organization permissions to resources that are stored in a different AD environment – in different forests.

Within the context of **Microsoft Intune,** it's possible for Intune to manage Windows devices that are both Hybrid Entra joined and Entra ID joined. Devices that are joined to AD DS and need to become available in Entra ID join as well are known as **Hybrid Entra ID join.** Before your business is ready to work natively in Entra ID, Hybrid Entra ID might be the best option to use as an interim solution.

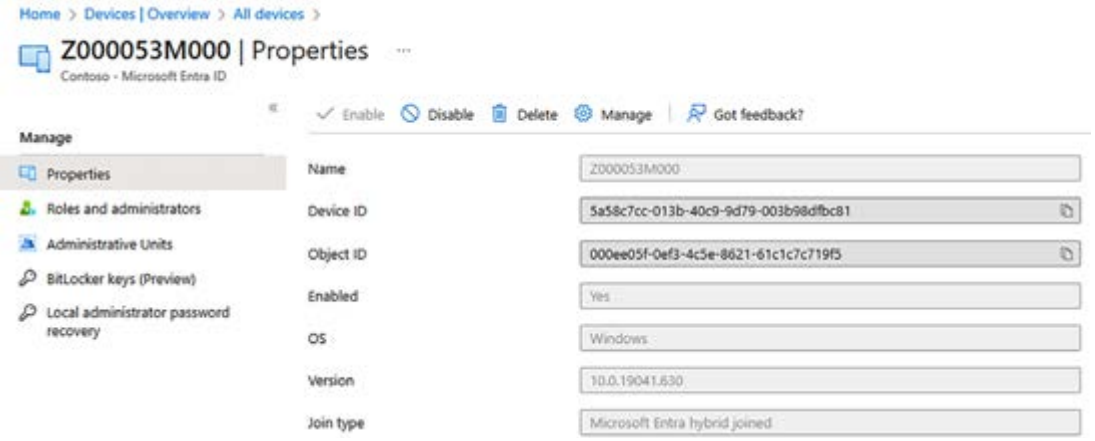


Figure 13.1: Microsoft Entra Hybrid joined

If your devices are enrolled into Entra ID directly and listed in **All Devices** within Microsoft Intune, you can see the Entra ID domain properties in your Windows 11/10 Enterprise **Settings** menu.

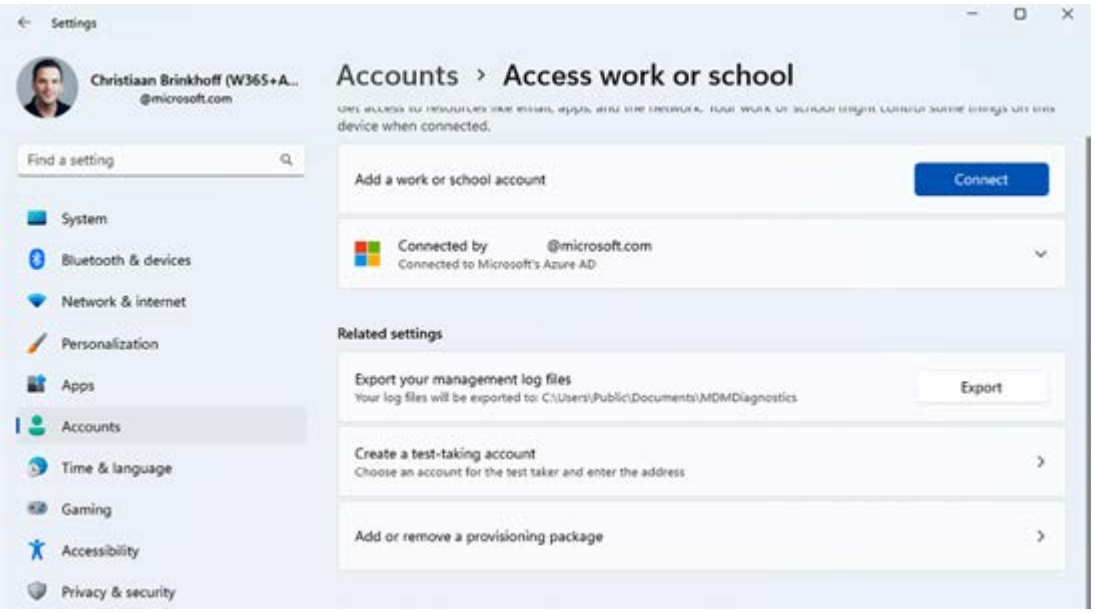


Figure 13.2: Access work or school

Devices can be in different states, but common for them all is that you can see them in the Settings App under **Accounts | Access work or school**.

Let's look at Entra ID next.

Entra ID

Previously known as **Azure Active Directory** (**Azure AD**), Microsoft Entra ID is a cloud-based directory and identity management service provided by Microsoft. It's a multi-tenant service that amalgamates core directory services, application access management, and identity protection into one comprehensive solution.

Microsoft Entra ID offers several key features:

- **Secure adaptive access:** This feature safeguards access to resources and data with robust authentication and adaptive access policies that are risk-based, without compromising the user experience.
- **Seamless user experiences:** It offers a quick and easy sign-in experience across your multicloud environment, which not only keeps your users productive but also reduces the time spent managing passwords, thereby enhancing productivity.
- **Unified identity management:** It allows you to manage all your identities and access to all your applications in one central location, irrespective of whether they're in the cloud or on-premises, thereby improving visibility and control.
- **Comprehensive capabilities:** It includes app integrations**, single sign-on** (**SSO**), passwordless and **Multifactor Authentication** (**MFA**), Conditional Access, identity protection, Privileged Identity Management, end user self-service, and a unified admin center.

Microsoft Entra ID is a market leader in managing directories, enabling access to applications, and protecting identities. It's currently being used by more than 300,000 organizations.

Let's look at Entra ID join.

Entra ID join or Hybrid Entra ID – What's the best option?

Entra ID join

Entra ID Join is a functionality that enables devices to be directly joined to Microsoft Entra ID, necessitating an organizational account for device sign-in. This feature is adaptable for both cloud-only and hybrid organizations and can be implemented for all users within an organization.



Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra Hybrid join devices isn't recommended, including through Autopilot. Source: `https://learn.microsoft.com/en-us/autopilot/windows-autopilot-hybrid`.

The key features of Microsoft Entra ID Join include:

- Providing **Single Sign-On** (**SSO**) access to resources both in the cloud and on-premises
- Enabling Conditional Access via **Mobile Device Management** (**MDM**) enrollment and compliance evaluation
- Offering Self-service Password Reset and Windows Hello PIN reset capabilities on the lock screen

Microsoft Entra ID Join is versatile and can be used in a variety of situations, such as when transitioning to a cloud-based infrastructure using Microsoft Entra ID and MDM like Intune, or when there is a need to manage mobile devices like tablets and phones. It's particularly useful when your users primarily need to access Microsoft 365 or other SaaS apps integrated with Microsoft Entra ID.

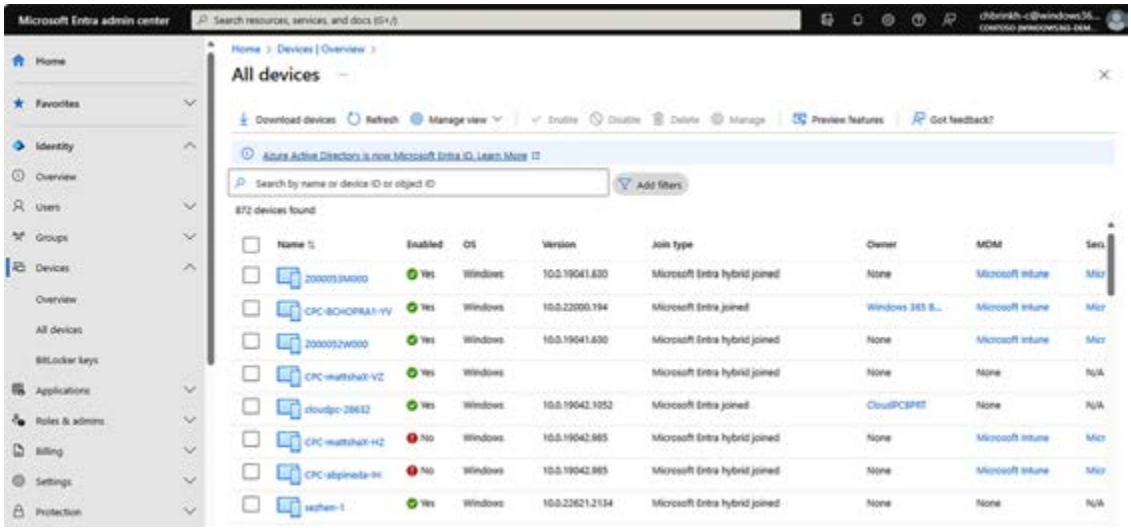


Figure 13.3: Entra admin center devices

To further secure and control Microsoft Entra ID joined devices, administrators can use **Mobile Device Management** (**MDM**) tools like Microsoft Intune or engage in co-management scenarios using Microsoft Configuration Manager. These tools allow for the enforcement of organization-required configurations, such as mandating storage encryption, setting password complexity rules, and managing software installation and updates.

Hybrid Entra ID join

Organizations that already have Active Directory set up can leverage some of the features offered by Microsoft Entra ID through the use of Microsoft Entra Hybrid joined devices. These devices are simultaneously connected to your local Active Directory and registered with Microsoft Entra ID.

It's important to note that Microsoft Entra Hybrid joined devices need periodic network access to your on-site domain controllers. Without this access, the devices may become inoperable. If this is a potential issue, you might want to think about using Microsoft Entra Join for your devices.

This could be a more suitable option if maintaining a constant network connection to your on-site domain controllers is challenging.

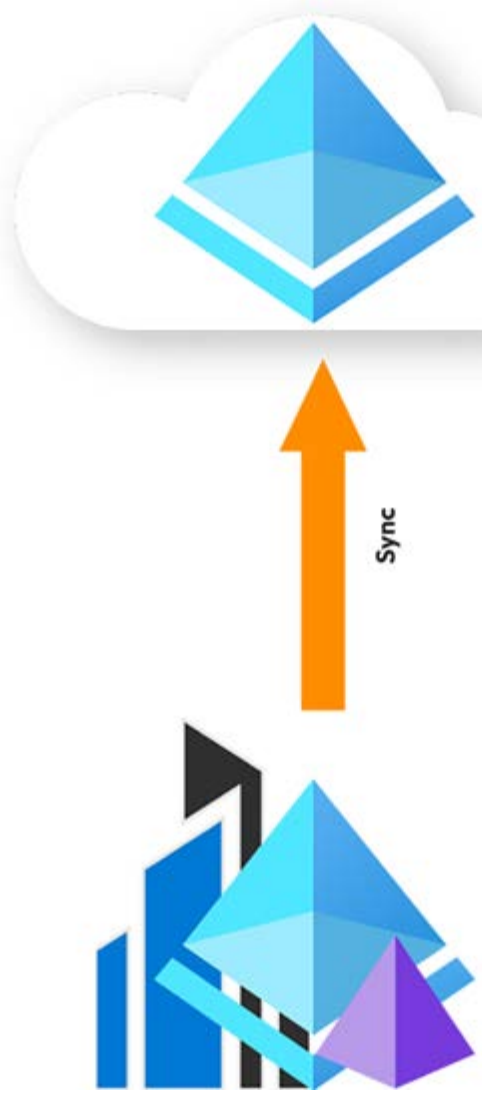


Figure 13.4: Entra Connect

To use Hybrid Entra ID, you must replicate your on-premises environment to bring/sync your identities and devices to Entra ID. You do that with the Microsoft Entra ID Connect software.

The software has been built on **Microsoft Identity Management** (**MIM**) and is preconfigured with all the configuration items to replicate your on-premises users, groups, and devices to Entra ID.

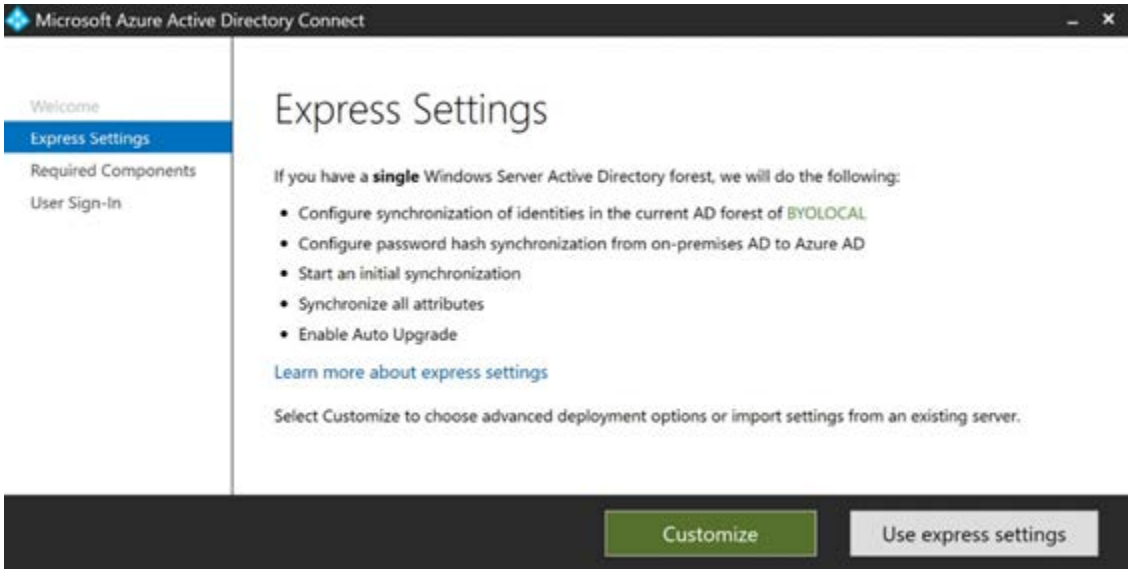


Figure 13.5: Microsoft Entra ID Connect – Express Settings

If you have configured Entra ID Connect in the past, you must change the configuration to Entra ID Joined for services such as Windows 365. Hybrid Entra ID could also be beneficial in the following alternative scenarios:

- You have Win32 apps deployed to these devices that rely on AD machine authentication.
- You want to continue to use Group Policy to manage device configuration.
- You want to continue to use existing imaging solutions to deploy and configure devices.
- You must support down-level Windows 7 and 8.1 devices in addition to Windows 10/11.

Make sure that the server where you configure Entra ID Connect can connect to all the following URLs:

- `https://enterpriseregistration.windows.net`
- `https://login.microsoftonline.com`
- `https://device.login.microsoftonline.com`
- `https://autologon.microsoftazuread-sso.com`

Follow these steps to align with the prerequisites of the service. For physical PCs, do the following:

1. Go to your Entra ID Connect server, most likely running on-premises in your own private cloud data center environment.
2. Open the Microsoft Entra ID Connect program.
3. Open the **Configure device options** task.

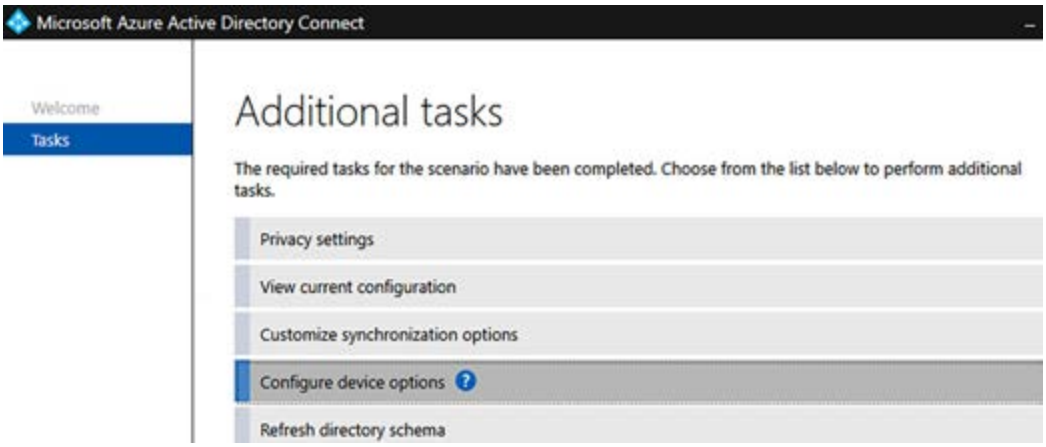


Figure 13.6: Configure device options

4. Verify that you are the owner of this Entra ID tenant by logging on with your organization's Global Administrator account.

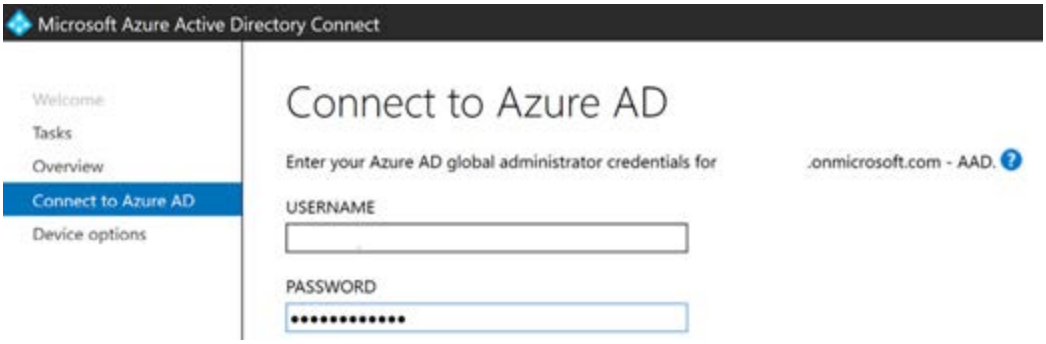


Figure 13.7: Connecting to Entra ID

5. After that is done, you will be asked to change the device options of your Entra ID configuration. Change this to **Configure Hybrid Azure AD join**.

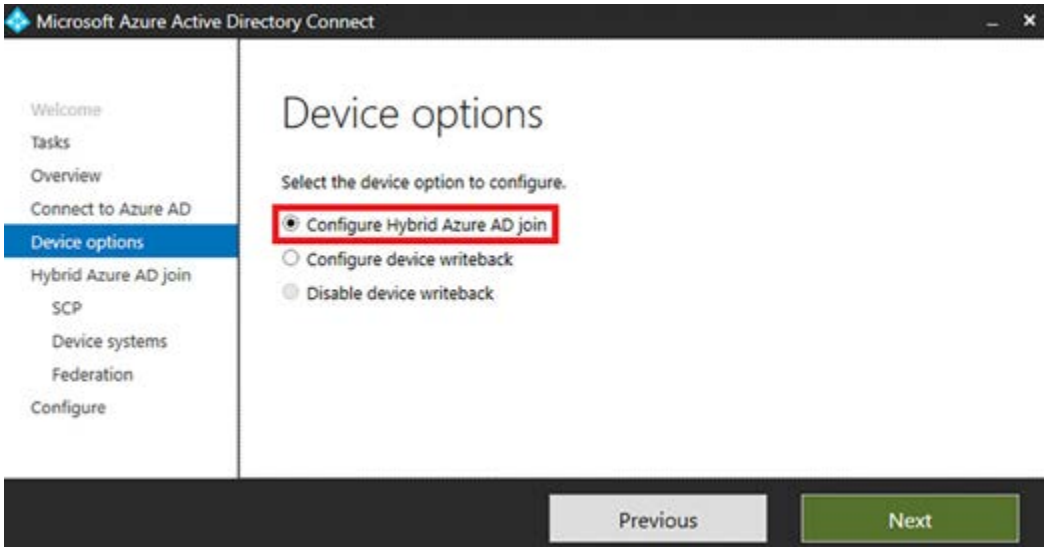


Figure 13.8: Configure Hybrid Entra ID join

6. Make sure to select the **Windows 10 or later domain-joined devices** option.



Figure 13.9: Device operating systems

7. After clicking **Next**, you must configure the **service connection point** (**SCP**) to your AD forest.

   You must click on the green **Add** button to add the right Enterprise Administrator credentials of your on-premises AD to the Entra ID authentication service.

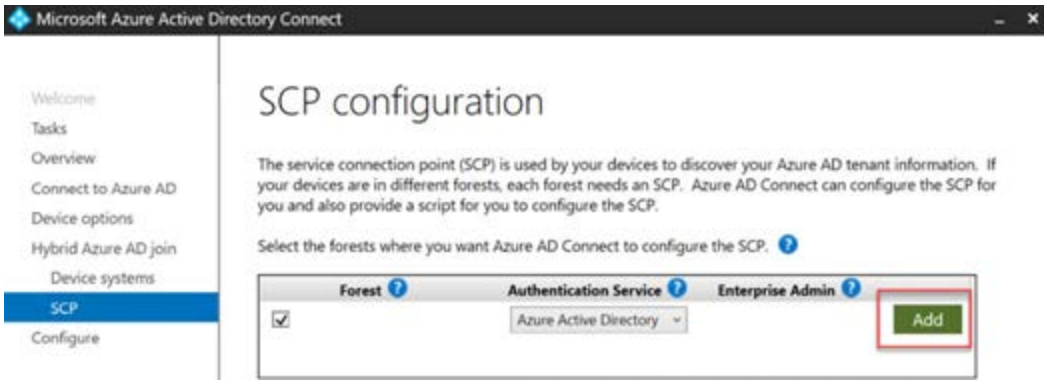


Figure 13.10: SCP configuration

8. Once done, click the **Next** button.

   You are now ready to change your Entra ID Connect configuration to a Hybrid Entra ID.

9. Click **Configure** to start the configuration.

Next, let's talk about Entra ID users and groups.

Entra ID users

Entra ID users include the account settings of a user in your organization and only live in the Microsoft Azure cloud. Creating and deleting users can be done by using either the Entra ID Global Administrator role or an account that has the account administrator **role-based access control** (**RBAC**) role assigned.

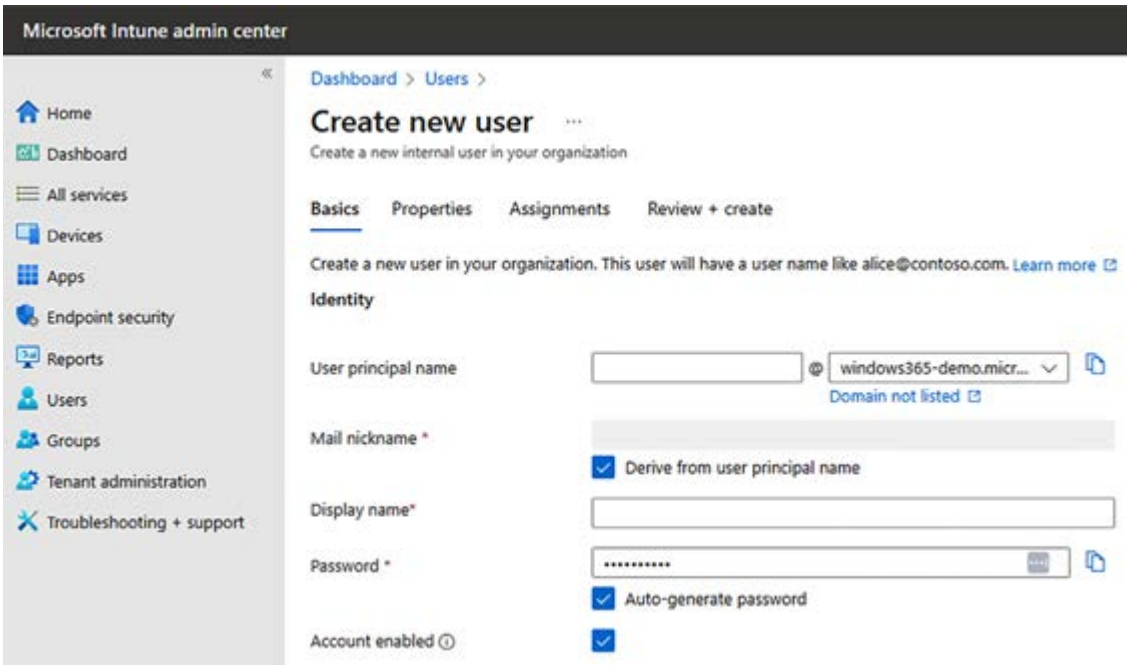


Figure 13.11: New user in the Microsoft Intune admin center

Creating new users directly in Entra ID is for cloud-only identities; hybrid identities still need to be created in the on-premises AD and synced to Entra ID with Entra ID Connect. Let's look at Entra ID guest users next.

Entra ID guest users

Guest user accounts are designed to collaborate with other organizations outside of your Entra ID tenant environment without creating a normal Entra ID user account that contains your organization's domain. One example is to allow access to a SharePoint site. If an end user has permission to share documents in OneDrive for Business, it can also be done with a guest user.

Be aware that a guest user cannot enroll a device into Entra ID or Microsoft Intune.

In the **Create a new user** workflow, the IT admin can choose to invite a user instead of creating one in the corporate Entra ID, as seen in this workflow:



Figure 13.12: Inviting guest users

In the **Invite user** workflow, the IT admin can also assign groups or roles in Entra ID. This means that a guest user can be assigned the role of Intune administrator, so you can give the role to an external consultant, as an example.

Let's look at different options for groups in Entra ID next.

Entra ID group types

There are two types of Entra ID groups, as follows:

- **Security:** This is the most commonly used type as it is used to add members to a group to gain access to a folder share, applications, RBAC, a security policy, or a cloud desktop environment.
- **Microsoft 365:** This is the group type used within other Microsoft cloud services, such as Exchange Online and SharePoint, to collaborate better. This group type also allows customers to share access to members outside the organization's Entra ID tenant environment.

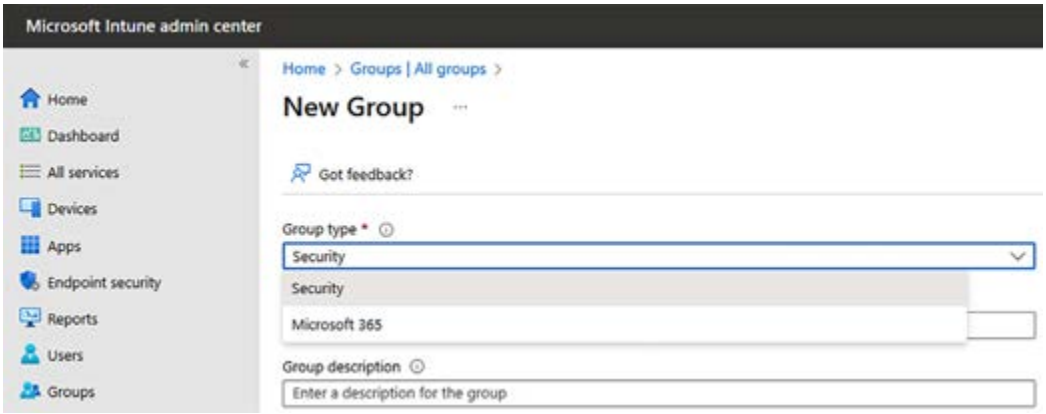


Figure 13.13: Creating a new group

Security groups can be used for both users or devices but not a mix. Next, we will look at the different membership types.

Entra ID group membership types

In the previous section, we explained the differences in the types of Entra ID groups. There are three ways to make users or devices members of an Entra ID group:

- **Assigned:** This is the most common way of assigning access to a specific group. You add specific users to an Entra ID group to gain access, for example, to a security policy.
- **Dynamic user:** This type makes it possible to automatically add users to a group based on conditions that you define. There is no interaction needed to add – as well as remove – users to the Entra ID group when the user no longer meets the requirements to be part of the group.
- **Dynamic device:** This type is somewhat the same as the dynamic user membership type; however, it is used to automatically add or remove devices from the Entra ID group.

Pick the type that fits your use case best, as dynamic membership could provide a more scalable method for larger organizations. Dynamic groups are only supported as either the user or device type – not both.

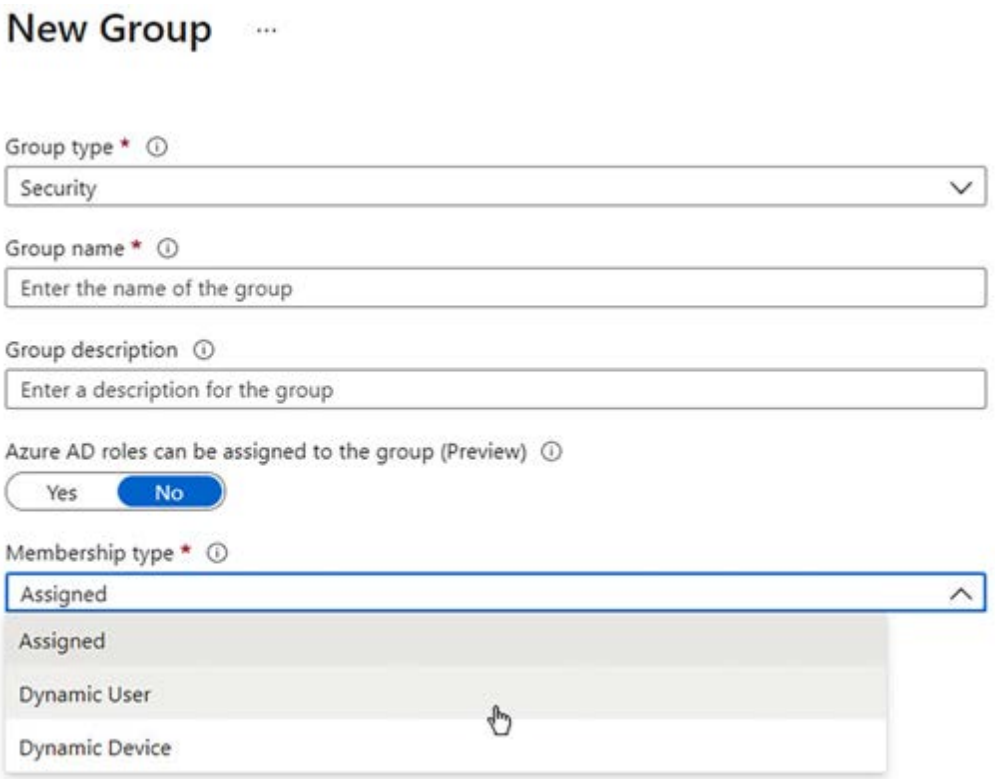


Figure 13.14: Creating a new group

Within the dynamic membership rules, you can create complex attribute-based rules to enable dynamic membership for groups, which you could use to add and remove users from the Entra ID group.

For example, you can add all users that have `@contoso.com` as `proxyAddresses` configured in Entra ID automatically by adding the following rule. You can imagine that any number of options will be available through this approach.

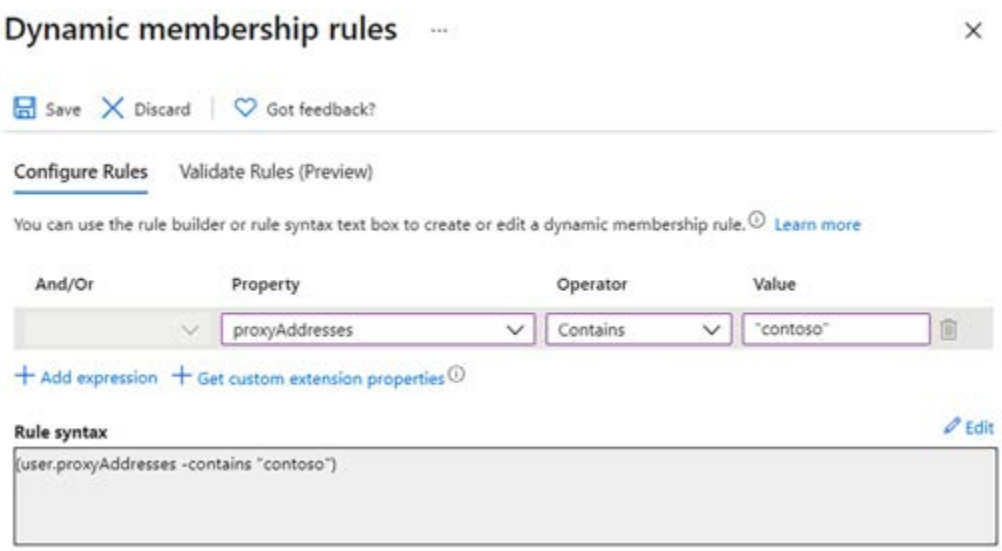


Figure 13.15: Dynamic membership rules

You can easily test the expressions as well with the **Validate Rules** option now. If the validation turns red, it means that the user isn't part of the allowed filtering property and therefore will not be added to the Entra ID group dynamically:

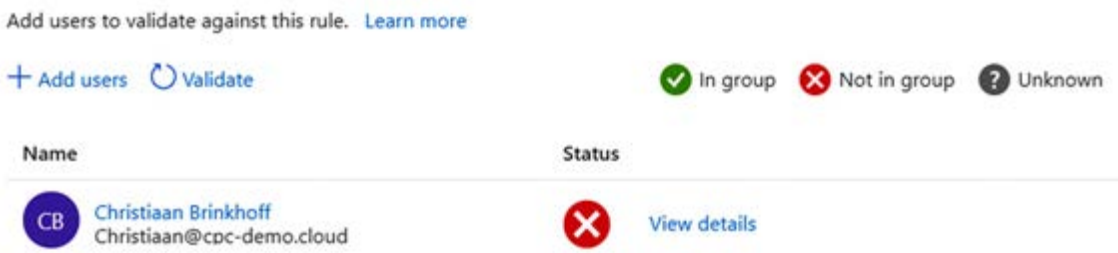


Figure 13.16: Dynamic rule validation

Dynamic groups can help you be more agile in your Microsoft Intune assignment. Dynamic devices have several attributes that can help group similar device types as one example.

Next, let's read about Conditional Access.

Conditional Access

Microsoft Entra Conditional Access is a powerful policy engine that plays a crucial role in enforcing security policies within organizations. Let's break it down.

What is it?

- Conditional Access is Microsoft's Zero Trust policy engine.
- It takes signals from various sources into account when making access decisions.
- Essentially, it's like a set of *if-then* statements:
    - If a user wants to access a resource (like Microsoft 365), then they must complete a specific action.
    - For example, if a user wants to access an application, they might need to perform multifactor authentication to gain access.

What are the common signals?

- **User or group membership**: Policies can be targeted to specific users or groups, allowing fine-grained control over access.
- **IP location information**: Organizations can define trusted IP address ranges for policy decisions.
- **Device attributes**: Specific platforms or device states can influence Conditional Access policies.
- **Application context**: Different applications can trigger distinct Conditional Access policies.
- **Risk detection**: Integration with Microsoft Entra ID Protection identifies and mitigates risky user behavior.
- **Microsoft Defender for Cloud Apps**: Monitors and controls user application access in real time.

What are the common decisions?

- **Block access**: The most restrictive decision
- **Grant access**: Less restrictive, but can require actions like multifactor authentication or a compliant device

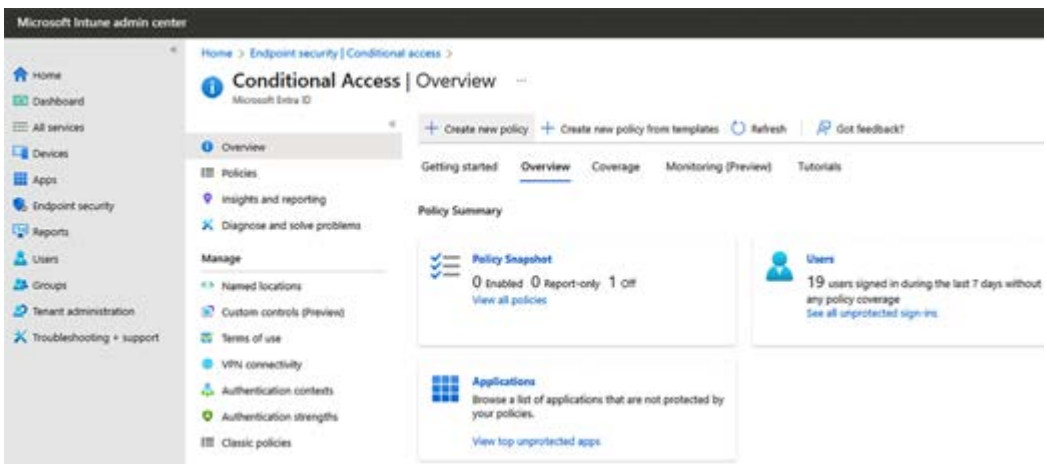


Figure 13.17: Conditional Access

Administrators must have two primary goals:

- Empower users to be productive wherever and whenever.
- Protect the organization's assets.

You can apply the right access controls when needed to keep your organization secure and stay out of your users' way when not needed with the help of Conditional Access policies.

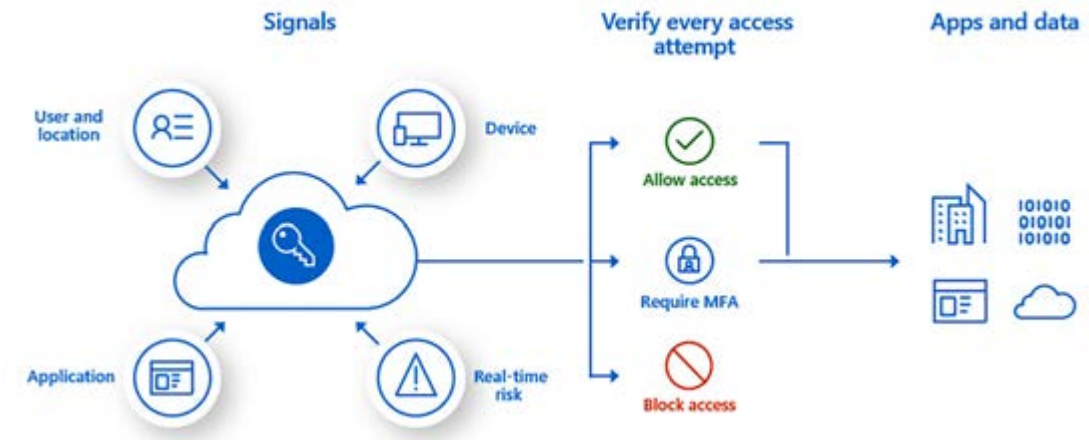


Figure 13.18: Conditional Access workflow

Next, we will look at user and group scoping in a Conditional Access policy.

Users and groups

Conditional Access allows you to control user access based on user and group assignments. The creation of a Conditional Access policy starts with filtering based on the following conditions:

- **None**
- **All users**
- **Select users and groups:**
    - **All guest and external users**
    - **Directory roles**
    - **Users and groups**

The following screenshot is an example of configuring filters based on Entra ID groups:

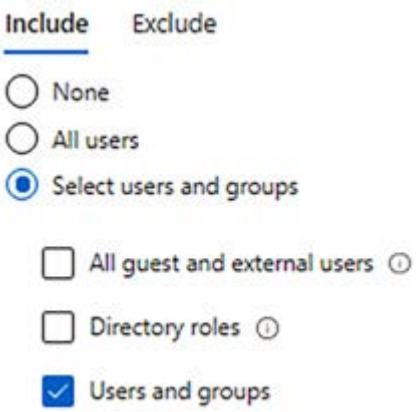


Figure 13.19: Including users and groups

Including and excluding users and group assignments can be configured to fit the access control your company needs.

Next, we will look at cloud apps in a Conditional Access policy.

Cloud apps

Cloud apps are Entra ID Enterprise applications that represent the Microsoft cloud or third-party applications. This could be, for example, Windows 365, AVD, a **Software as a Service** (**SaaS**) application, or Office 365 services.

To enforce different Conditional Access settings per cloud app(s), you can create different policies that only apply to that specific application to customize access:



If you want to enable Azure MFA for **Windows 365**, you need to select Windows Cloud Login, Windows Virtual Desktop, and Windows Virtual Desktop Client.

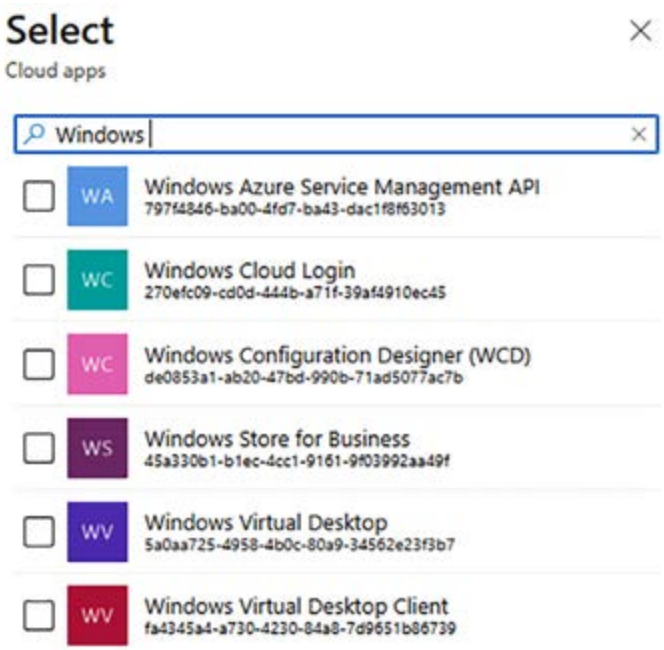


Figure 13.20: Selecting cloud apps

Cloud apps are usually named after the service; otherwise, you have to select them according to the right app ID, such as `0af06dc6-e4b5-4f28-818e-e78e62d137a5`.

Aside from filtering on cloud apps, you could also apply Conditional Access settings during actions, for example, the process of registering and joining devices to Microsoft Intune. You must then select user actions instead of cloud apps:

- **Register security information**
- **Register or join devices**

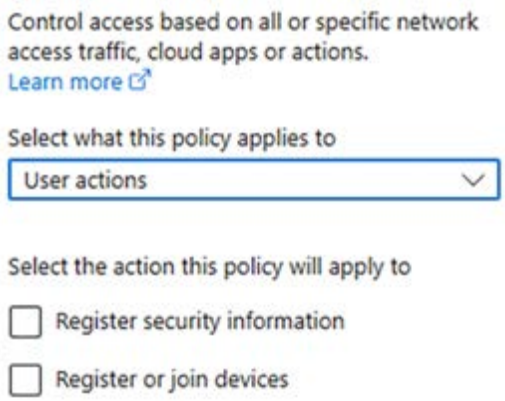


Figure 13.21: User actions

Next, we will look at conditions in a Conditional Access policy.

Conditions

There are four different types of conditions to configure:

- **Device platforms**: Control user access from different device platforms; for example, this policy should only apply when users log on from Android, Windows, macOS, iOS, or a Windows phone.

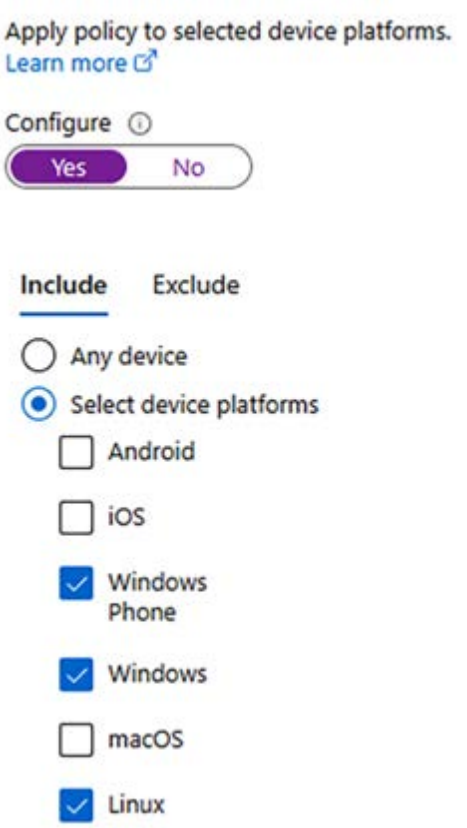


Figure 13.22: Including/excluding a platform

- **Locations:** Control user access based on their physical location, for example, based on public IP allow-listing.

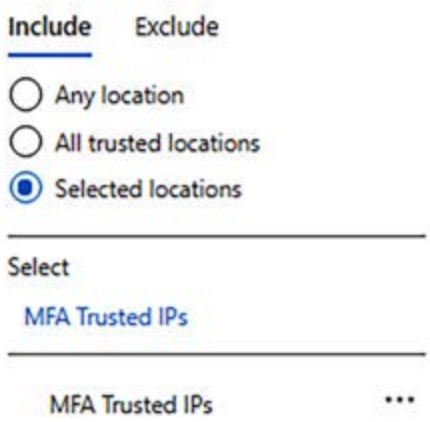


Figure 13.23: Include/exclude locations

You can configure IP authorization – IP lists in **Conditional Access** – in the **Named locations** menu.

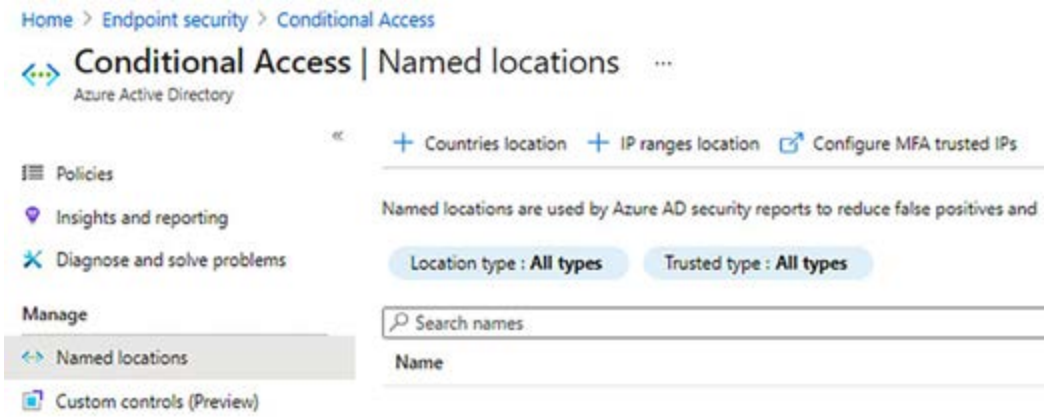


Figure 13.24: Conditional Access – Named locations

- **Client apps**: Control user access to target specific client applications not using modern authentication.

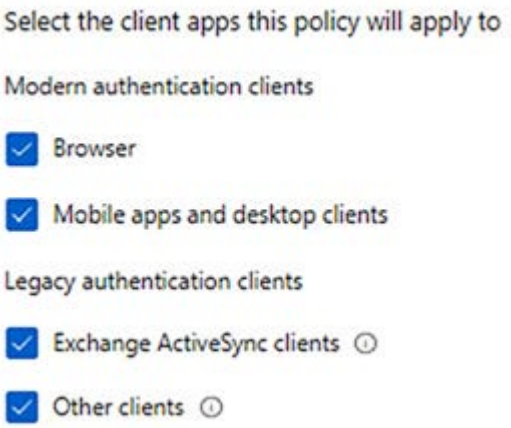


Figure 13.25: Select the client apps this policy will apply to

- **Device state**: Control user access when the device the user is signing in from is not Entra ID or marked as compliant.

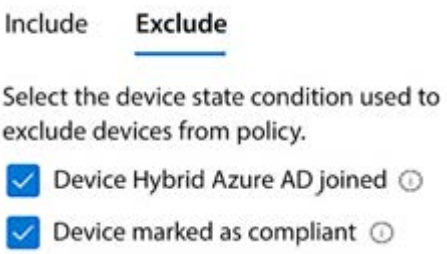


Figure 13.26: Excluding a device state

After assignments have been configured, you can continue to the access control.

Grant

You can select the following options as Conditional Access grant settings, of which MFA is the most common one to use:

- **Require MFA**: Users must complete additional security requirements such as a phone call or text.
- **Require device to be marked as compliant**: The device must be Intune-compliant. If the device is non-compliant, the user will be prompted to bring the device under compliance.
- **Require Hybrid Entra ID Joined device**: Devices must be Hybrid Entra ID Joined to get access.
- **Require approved client app**: Device must use these approved client applications.
- **Require app protection policy**: The devices that you connect from must use policy-protected apps.

You could also select multiple controls, to force either multiple requirement options or one of multiple options, to provide access if multiple endpoint scenarios apply:

- **Require all the selected controls**
- **Require one of the selected controls**



When selecting MFA and devices marked as compliant, you could lock yourself out, so please be careful!

Grant access can be configured to have either all or some controls.

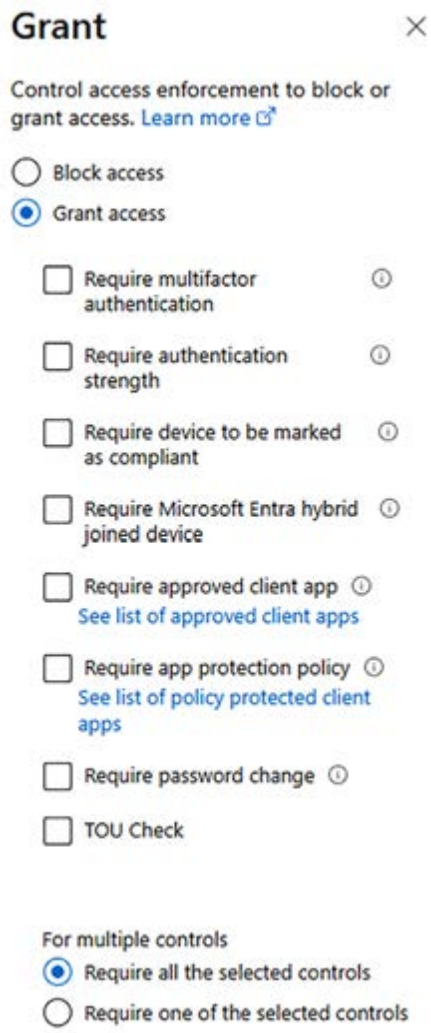


Figure 13.27: Grant access

MFA should be mandatory; add other settings as you like, for example, controlling access from devices that aren't Microsoft Intune-managed.

Control user access based on session controls to enable limited experiences within specific cloud applications:

- **Use app enforced restrictions**: App-enforced restrictions might require additional admin configurations within cloud apps. The restrictions will only take effect for new sessions.
- **Use Conditional Access App Control**: Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the cloud app security portal to further refine filters and set actions to be taken on a user.
- **Sign-in frequency**: This is the time period before a user is asked to sign in again when attempting to access a resource. The default setting is a rolling window of 90 days, that is, users will be asked to re-authenticate on the first attempt to access a resource after being inactive on their machine for 90 days or longer.



This setting could be beneficial in enforcing MFA every hour on **bring-your-own-device** (**BYOD**) devices to ensure that access expires after that time!

- **Persistent browser session**: A persistent browser session allows users to remain signed in after closing and reopening their browser window:



Persistent browser session only works correctly when **All cloud apps** is selected.

  - This does not affect token lifetimes or the sign-in frequency setting.
  - This will override the **Show option to stay signed in** policy on company branding.
  - **Never persistent** will override any persistent SSO claims passed in from federated authentication services.
  - **Never persistent** will prevent SSO on mobile devices across applications and between applications and the user's mobile browser.

- **Require token protection for sign-in sessions (Preview)**: A secure sign-in session requires all long-lived tokens (the Microsoft Entra session cookie and refresh token) to be bound to the device using software key binding or hardware security module binding where available.
- **Use Global Secure Access security profile**: Use this option to apply a policy profile for Global Secure Access targeted resources.

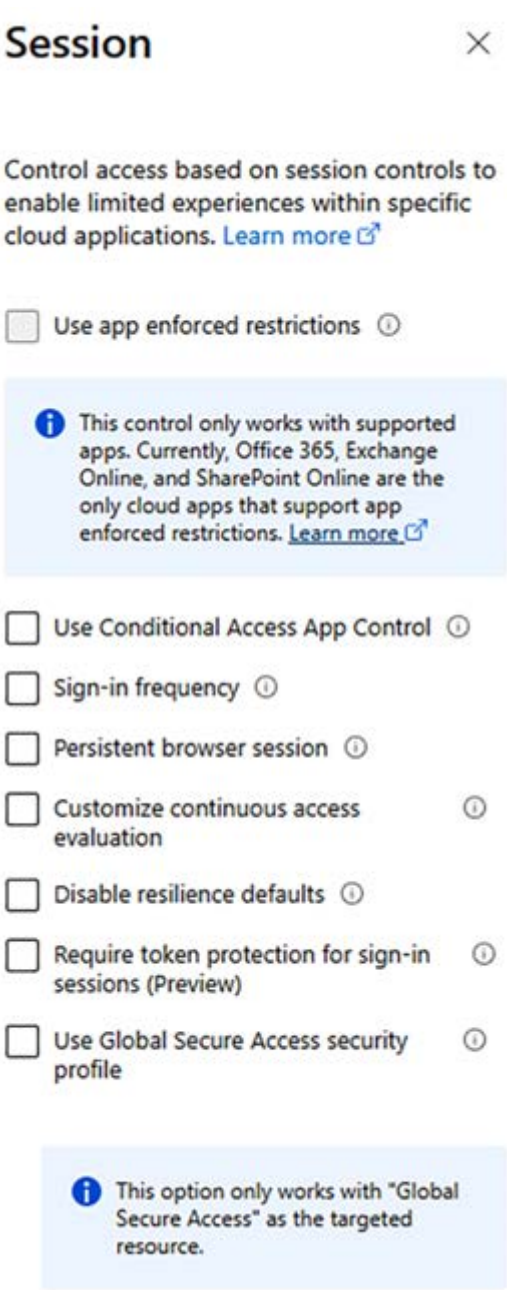


Figure 13.28: Session control

This concludes the walk-through of the Conditional Access policies that you can configure to secure your corporate data. Next, we will show an option to prevent users from carrying out Entra ID device registration on their BYOD devices.

Preventing users from carrying out Entra ID device registration

To block your users from adding additional work accounts to your corporate domain-joined, Entra ID joined, or Hybrid Entra ID Joined Windows devices, enable the following registry key: `HKLM\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin, "BlockAADWorkplaceJoin"=dword:00000001`.

This registry key can also be used to block domain-joined machines from inadvertently getting Entra ID registered with the same user account:

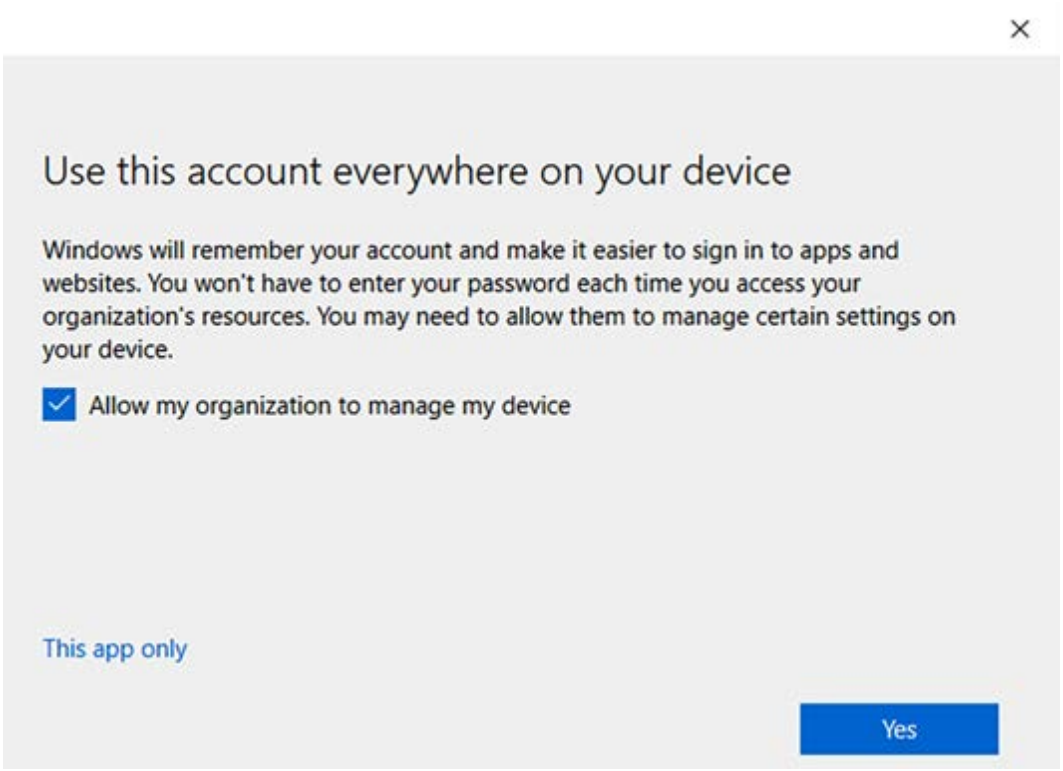


Figure 13.29: Use this account everywhere on your device

There is no central way to prevent a user from registering their BYOD device in Entra ID. If Entra ID automatic MDM enrollment is configured and the box for **Allow my organization to manage my device** is checked, the device will be enrolled into Microsoft Intune. Next, we will take a look at **Self-service Password Reset** (**SSPR**).

Self-service Password Reset

The SSPR feature allows businesses to give users the ability to reset their own passwords without any interaction with the service desk. This could massively reduce the number of support tickets in your organization as most users can recover themselves.

When a user enters their password too many times incorrectly, the account will go into a locked state. But with the SSPR service, the end user can still change the password, and here, they will be prompted for MFA during that process.



Before users can unlock their account or reset a password, they must register their contact information.

SSPR requires an Entra ID Premium P1 license, which comes with Microsoft 365 E3 or higher. Follow these steps to enable SSPR:

1. You must go to the Microsoft Entra admin center (`https://entra.microsoft.com`) to activate the feature.
2. In the **Protection** section, you will find **Password reset**.

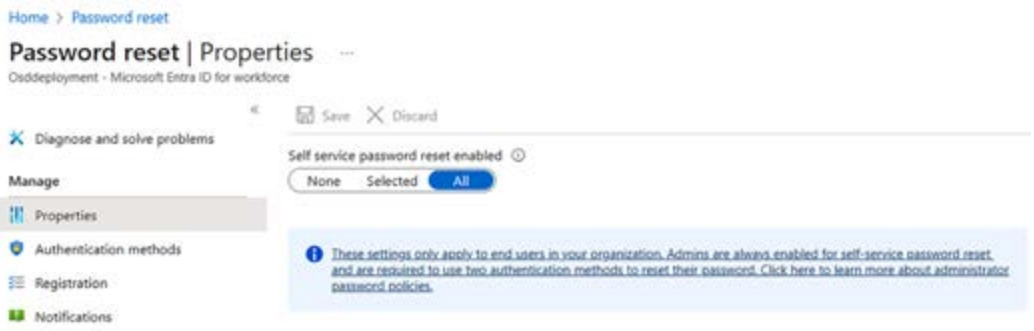


Figure 13.30: Self service password reset enabled

It's also possible to make SSPR available for Entra ID group members only via the **Selected** option in the menu.

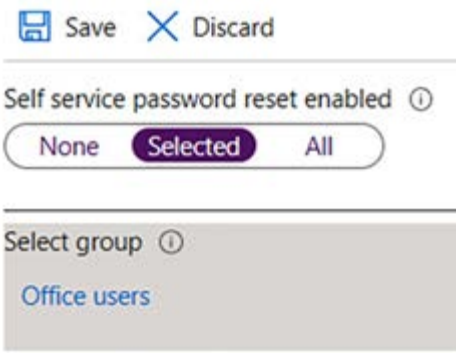


Figure 13.31: Password reset – selecting a group for scoping

Next, we will take a look at Entra ID password protection.

Entra ID password protection

Azure MFA keeps most intruders out – and proactively prevents other people from getting access to your environment with only the password. This isn't enough, as there are more Microsoft services to leverage in order to secure your user accounts...

Avoid bad passwords with the Entra ID password protection feature. With Entra ID password protection, default global banned password lists are automatically applied to all users in an Entra ID tenant. You can define entries in a custom banned password list to support your own business and security needs.

Adding this feature would assure you, as an IT administrator, that the most common passwords – which are no different every year – stay in the past!

You can find the **Password protection** feature under **Authentication methods** in the Entra admin center. You can also change the lockout thresholds here.

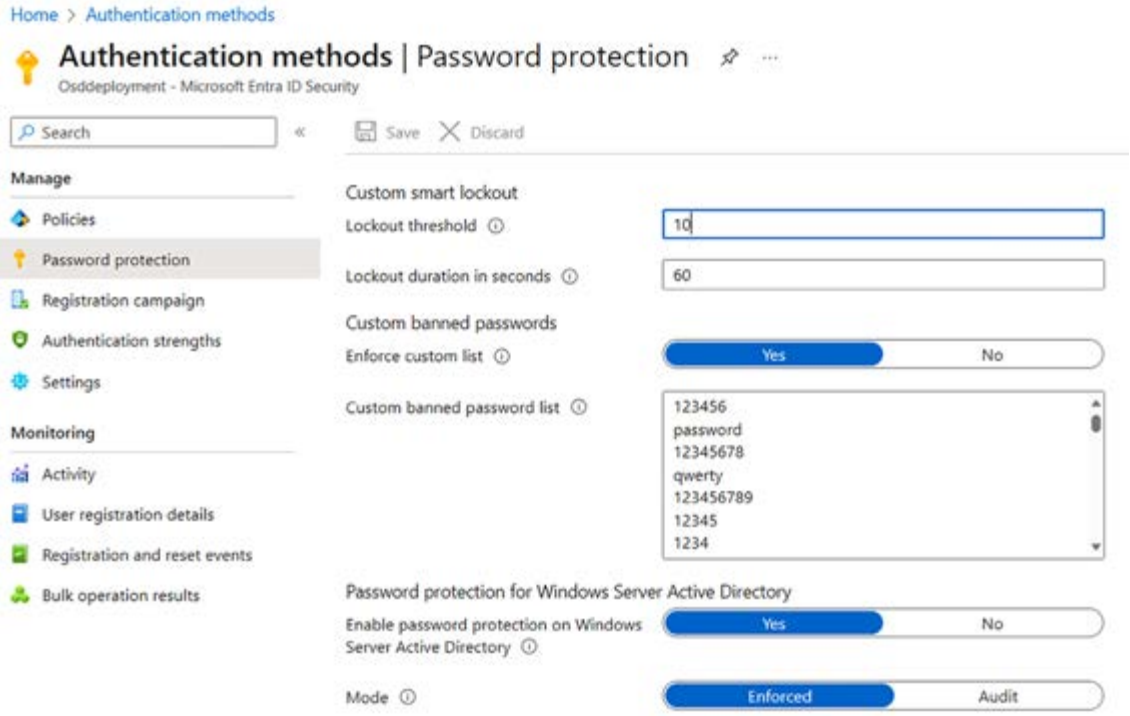


Figure 13.32: Password protection



Password protection requires you to have Entra ID Premium P2.

Next, we will look at passwordless authentication.

Passwordless authentication

While reading the previous section, you might have thought, what about passwordless sign-in authentication? Good point!

Microsoft aims to make setting passwords easier; their strategy is a four-step approach where we deploy replacement offerings, reduce the password surface area, transition to passwordless deployment, and, finally, eliminate passwords.

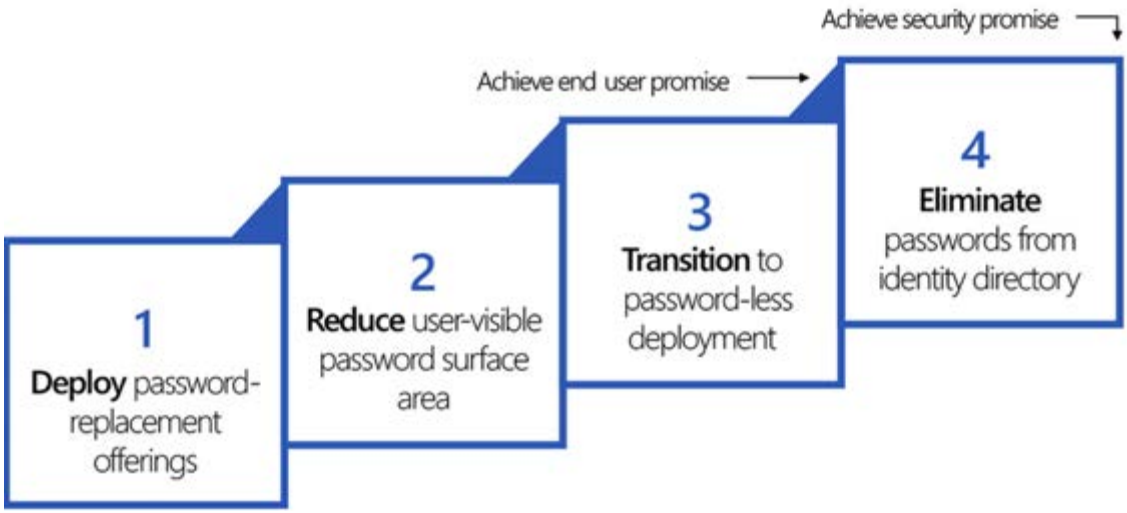


Figure 13.33: Passwordless phases

Passwordless authentication is a way to log on to your Windows Enterprise endpoint without entering your password. One of the most common approaches to do this is via a so-called YubiKey security key. You have them for USB-C, USB, and other devices, such as an Apple device. Other options are to use text messages or the Microsoft Authenticator app.



Figure 13.34: YubiKey

Let's talk about the YubiKey. The end user experience looks very similar to how you normally log on to Windows. While you normally log on with either Windows Hello or your password, you can now select a USB key, as shown:

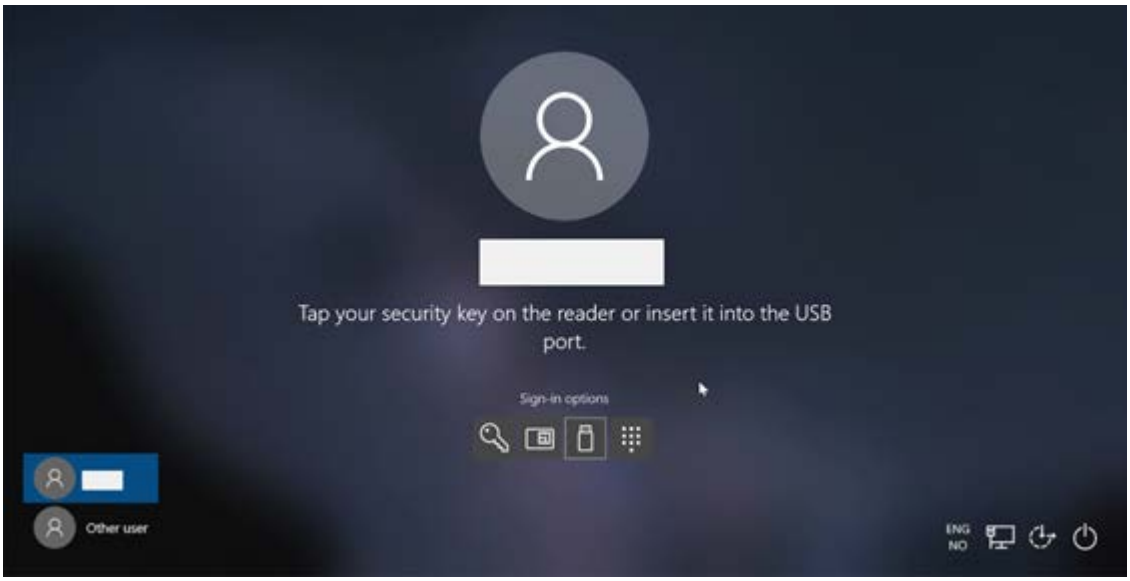


Figure 13.35: Windows sign-in options

After that, Windows will ask you to inject the security key into the USB port that holds the passphrase to log on to your Windows 10 device without a password.



Figure 13.36: FIDO2 authentication

First, you need to enable passwordless authentication in your Entra ID tenant.

Enabling passwordless authentication

To enable passwordless authentication, you have to go to the Microsoft Entra admin center. Then, follow these steps:

1. Go to **Protection**.
2. Open **Authentication methods**.
3. In the **Manage** menu, select **Authentication methods**.

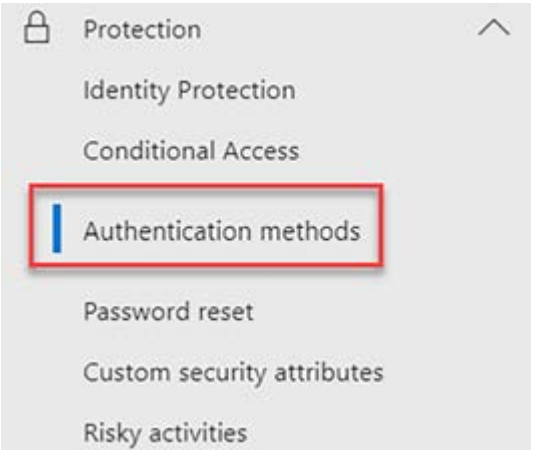


Figure 13.37: Authentication methods

4. Click on **FIDO2 Security Key**.

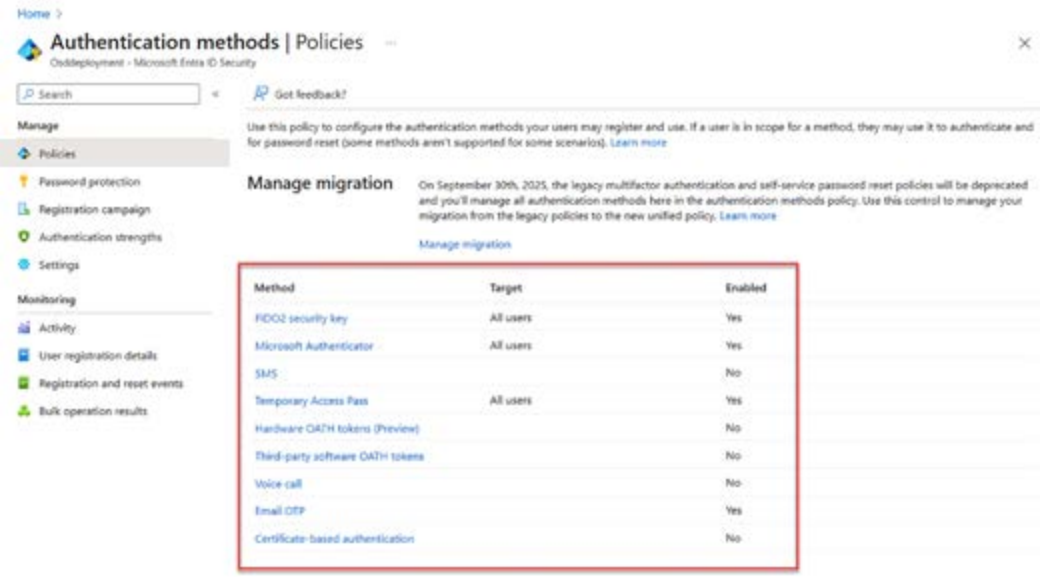


Figure 13.38: Authentication methods – Policies

5. Enable the settings for (at least) sign-in and strong authentication.



Figure 13.39: FIDO2 Enable and Target

6. Once you have enabled the use of FIDO2 keys, you also need to configure the **Configure** setting:

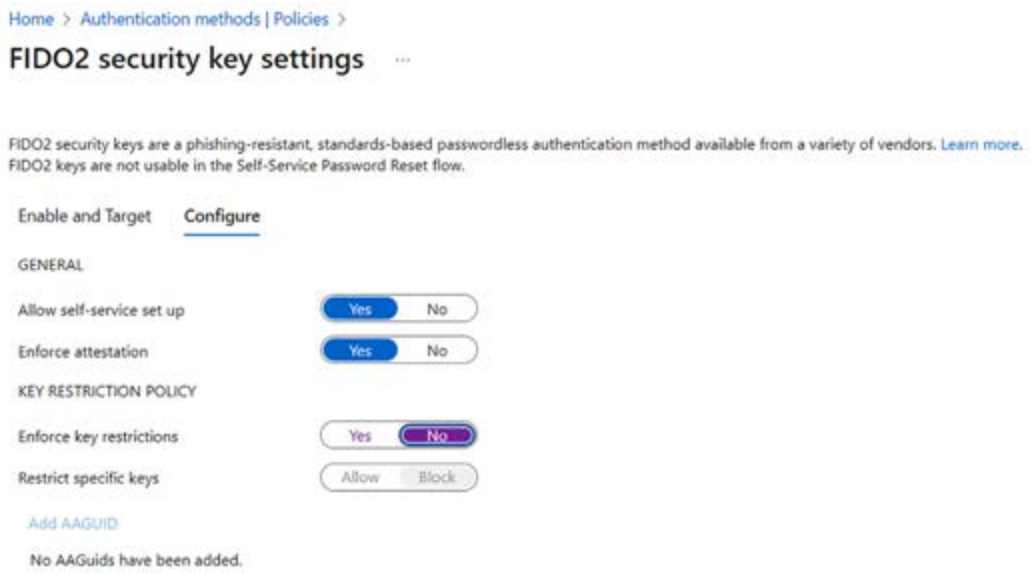


Figure 13.40: FIDO2 security key configuration

You can also use a key restriction policy to specify what FIDO2 keys your end users can leverage in your tenant, by entering an allow or block list of devices with an **Authenticator Attestation GUID** (**AAGUID**).

The FIDO2 specification requires each security key provider to provide an AAGUID during attestation. An AAGUID is a 128-bit identifier indicating the key type, such as the make and model.

You're now done with the prerequisites and are ready to use FIDO2 keys. You should see the following log-on screen for Entra ID while using passwordless authentication via the Microsoft Authenticator mobile application, all without entering the password.



Figure 13.41: Passwordless sign-in

Passwordless sign-in is more secure and the end user rarely has to enter their password anywhere. The end user can also change the sign-in option, to use a password instead.

Next, we will show a table of where the end user can leverage passwordless sign-in.

What is and isn't supported in each passwordless scenario

Microsoft's passwordless authentication methods enable different scenarios. The organizational needs, prerequisites, and capabilities of each authentication method need to be considered before selecting your passwordless authentication strategy.



There is no additional cost for passwordless authentication.

In the following table, you can see the options based on different scenarios:

Scenario	Phone authentication	Security keys	Windows Hello for Business
Computer sign-in: From an assigned Windows 10 device	No	Yes With biometric recognition and/or PIN	Yes With biometric recognition and or PIN
Computer sign-in: From a shared Windows 10 device	No	Yes With biometric recognition and/or PIN	No
Web app sign-in: From a user-dedicated computer	Yes	Yes Provided SSO to apps is enabled by computer sign-in	Yes Provided SSO to apps is enabled by computer sign-in
Web sign-in: From a mobile or non-Windows device	Yes	No	No
Computer sign-in: From a non-Windows computer	No	No	No

Table 13.1: Passwordless scenario

With Windows 11, you have the option to enable a passwordless experience with Intune – you need to create a settings catalog policy.

You find the policy under Authentication; the setting is called **Enable Passwordless Experience.** You need to set the value to **Enabled. The Passwordless experience will be enabled on Windows.**

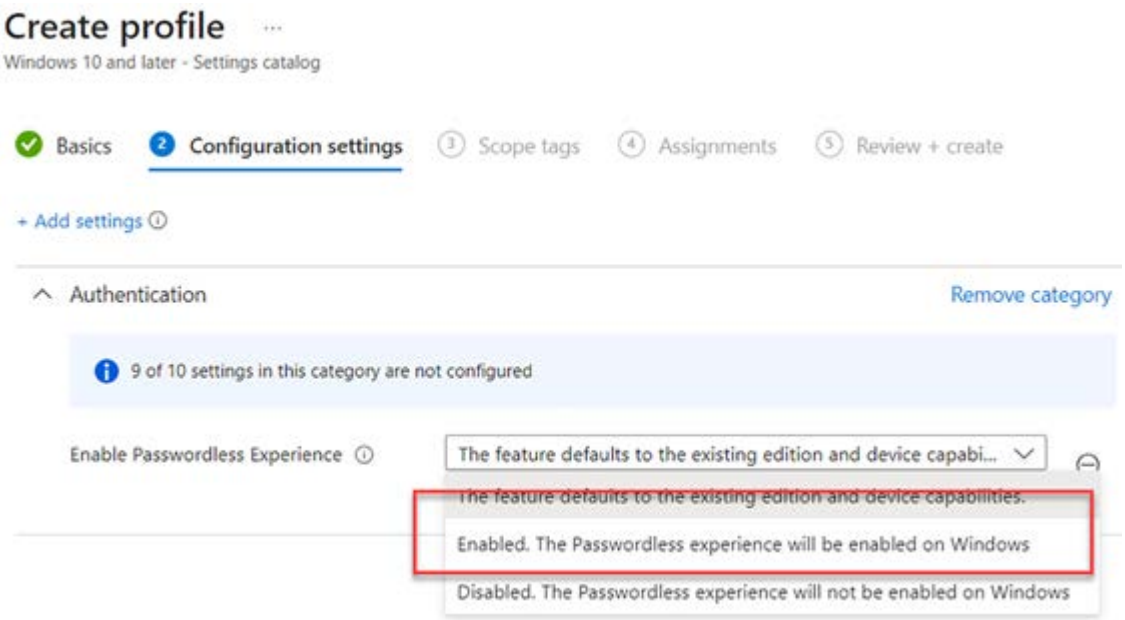


Figure 13.42: Passwordless policy

The requirements for a passwordless experience policy are as follows:

- Windows 11 22H2 with OS Build 22621.2361 or newer
- Device needs to be Entra Joined
- Needs to be Microsoft Intune Managed
- Needs to have the user enrolled with Windows Hello for Business or a FIDO2 security key

This concludes the section about passwordless sign-on. Next, we will cover passkeys.

Passkeys

Passkeys offer a more secure and user-friendly way to log in to websites and applications compared to traditional passwords. Unlike passwords, which require memorization and manual input, passkeys are securely stored on a device and can utilize the device's unlock features, such as biometrics or a PIN. This eliminates the need for additional sign-in challenges, making the authentication process quicker, safer, and more user-friendly.

Passkeys can be used with any applications or websites that support this feature, allowing you to create and sign in with Windows Hello. Once a passkey is established and saved with Windows Hello, you can use your device's biometrics or PIN for sign-in. Alternatively, a companion device like a phone or tablet can also be used for sign-in. In order to use passkeys, you would need to be licensed for any of the following Windows licenses.

Windows Pro/Pro Education/SE	**Windows Enterprise E3**	**Windows Enterprise E5**	**Windows Education A3**	**Windows Education A5**
Yes	Yes	Yes	Yes	Yes

Table 13.2: Supported Windows editions

How do passkeys work?

Microsoft, a founding member of the FIDO Alliance, has been instrumental in defining and implementing passkeys as a native feature within platform authenticators like Windows Hello. Passkeys adhere to the FIDO security standard, which is recognized by all major platforms. As part of the FIDO Alliance, leading tech companies like Microsoft are endorsing passkeys, and a growing number of websites and apps are incorporating passkey support.

FIDO protocols employ standard public/private key cryptographic methods to provide enhanced authentication. When a user signs up for an online service, their device generates a new key pair. The private key is securely stored on the user's device, while the public key is registered with the online service. To authenticate, the device must demonstrate that it holds the private key by signing a challenge. The private keys can only be used once they are unlocked by the user using the Windows Hello unlock factor (biometrics or PIN).

FIDO protocols are designed with a focus on user privacy, aiming to prevent online services from sharing information or tracking users across various services. Moreover, any biometric data used during the authentication process stays on the user's device and is not transmitted over the network or to the service.

How does it relate to passwords?

Passkeys offer several benefits over traditional passwords, including their user-friendly and intuitive design. Unlike passwords, passkeys are simple to generate, don't require memorization, and don't need to be protected. Furthermore, passkeys are unique to each website or application, preventing their reuse. They offer high security as they are stored solely on the user's devices, with only public keys stored by the service. Passkeys are designed to thwart attackers from guessing or obtaining them, making them resistant to phishing attempts where the attacker may try to deceive the user into revealing the private key. Passkeys are enforced by browsers or operating systems to be used exclusively for the appropriate service, eliminating the need for human verification. Lastly, passkeys enable cross-device and cross-platform authentication, meaning a passkey from one device can be used to sign in on another device.

How to enable passkeys

1. Open a **website** or **app** that supports passkeys.

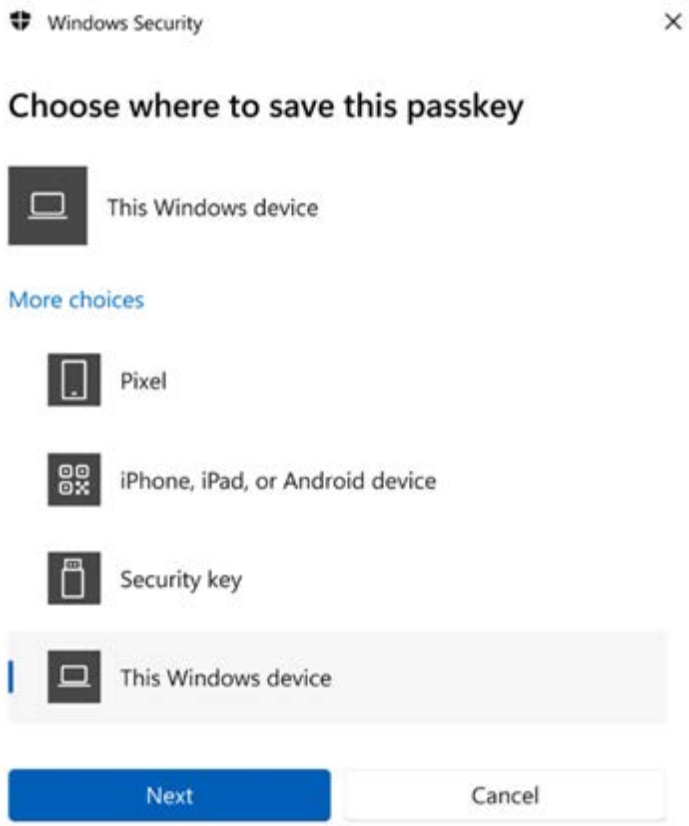


Figure 13.43: Choose where to save this passkey

2. Create a passkey from your account settings.



Figure 13.44: iPhone, iPad, or Android device

3. Choose where to save the passkey. By default, Windows offers to save the passkey locally if you're using Windows Hello. If you select the option **Use another device**, you can choose to save the passkey in one of the following locations:

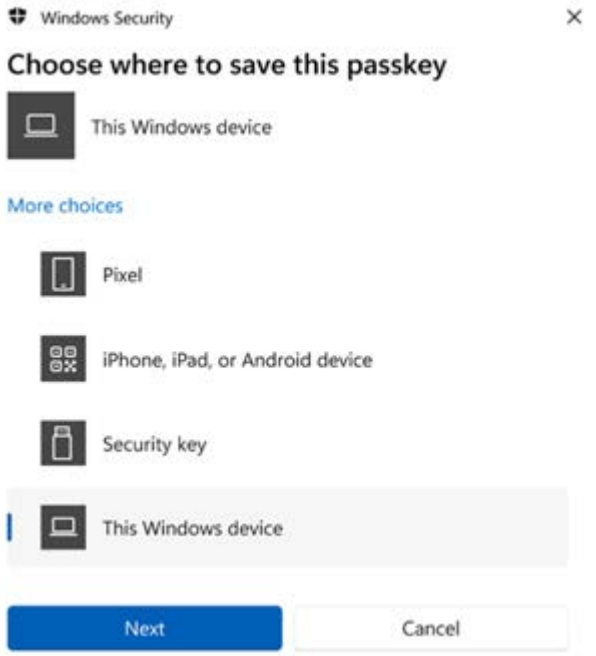


Figure 13.45: Passkey this Windows device

4. The passkey is saved to your Windows device. To confirm, select **OK**.

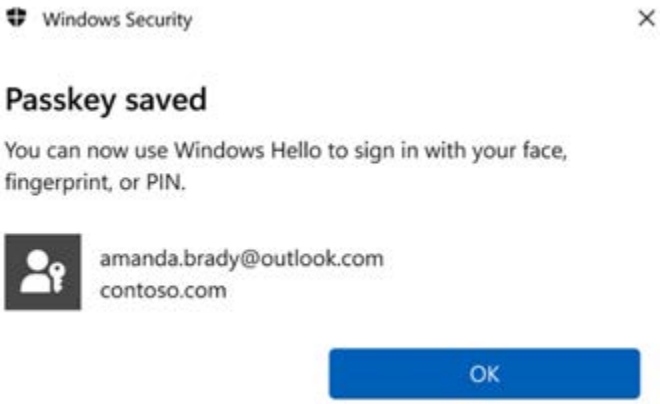


Figure 13.46: Passkey saved

Manage your passkeys

You can use the Settings App to view and manage passkeys saved for apps or websites. Select **Start** > **Settings** > **Accounts** > **Passkeys**.

A list of saved passkeys is displayed and you can filter them by name:

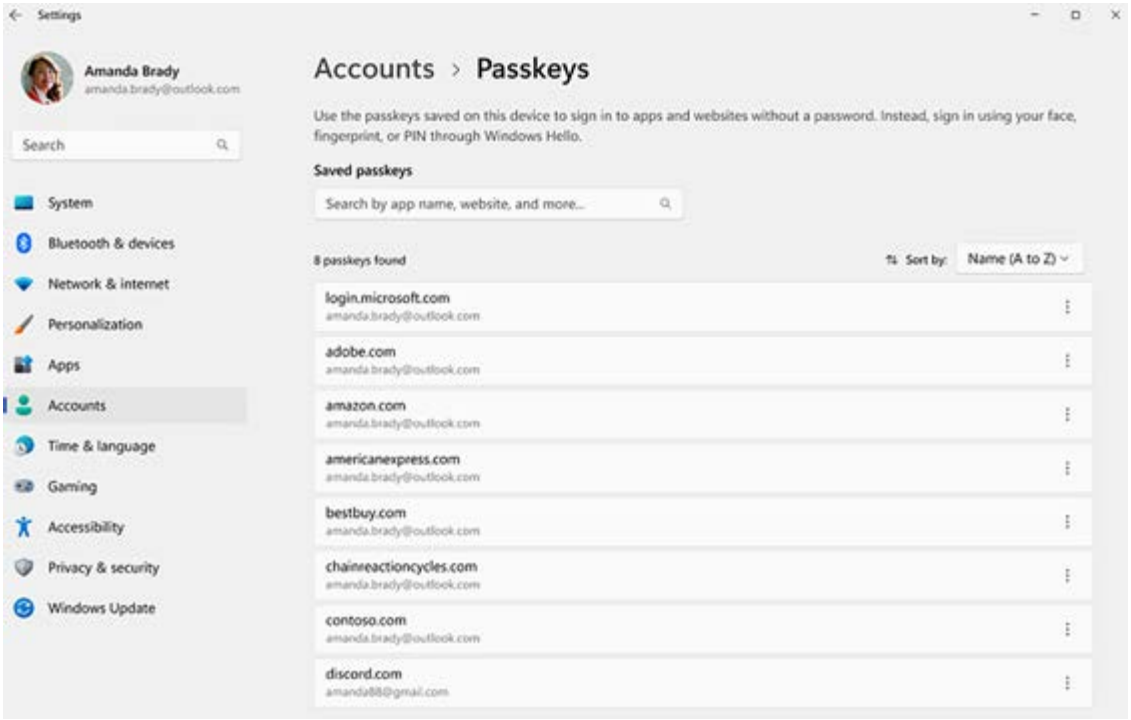


Figure 13.47: Windows settings passkey

If a passkey is locally stored and you access a website or app that supports passkeys, you will be automatically asked to use Windows Hello to sign in.

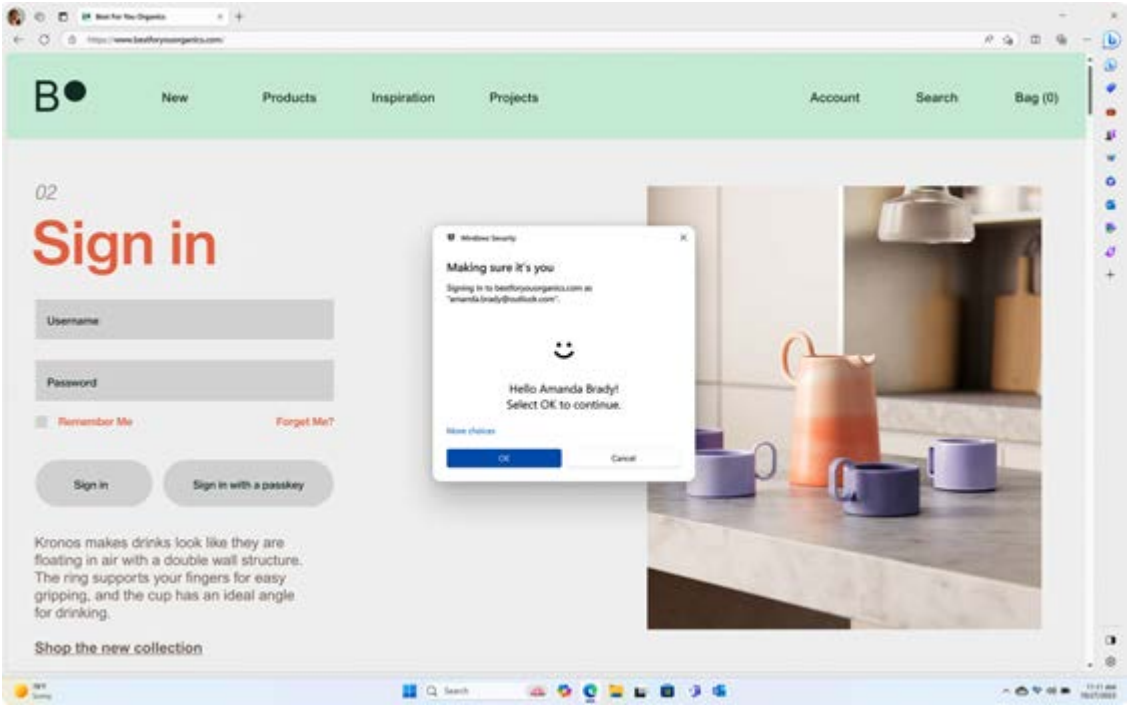


Figure 13.48: Website passkey

Let's talk about web sign-in now...

Web sign-in

Starting with Windows 11, version 22H2, and the KB5030310 update, a web-based sign-in experience is now available on devices joined to Microsoft Entra. This new feature, known as web sign-in, opens up new sign-in options and capabilities. If Windows Hello doesn't work for any reason, you can also use the Azure Authenticator app, or another alternative secure option.

Web sign-in, which is a credential provider, was first introduced in Windows 10, but it only supported **Temporary Access Pass** (**TAP**). However, with the launch of Windows 11, the scenarios and capabilities supported by web sign-in have been extended. For instance, users can now sign in using the Microsoft Authenticator app or a SAML-P federated identity.

Web sign-in is supported for the following Windows licenses.

Windows Pro/Pro Education/SE	Windows Enterprise E3	Windows Enterprise E5	Windows Education A3	Windows Education A5
Yes	Yes	Yes	Yes	Yes

Table 13.3: Support Windows editions

To use web sign-in, your devices must be configured with different policies. Review the following instructions to configure your devices using either Microsoft Intune or a **provisioning package** (**PPKG**). We will explain the Intune method.

1. You can easily **enable** web sign-in via the **Intune Settings catalog | Authentication policy**.
2. Ensure you check the box next to the **Enable Web Sign In** setting name.

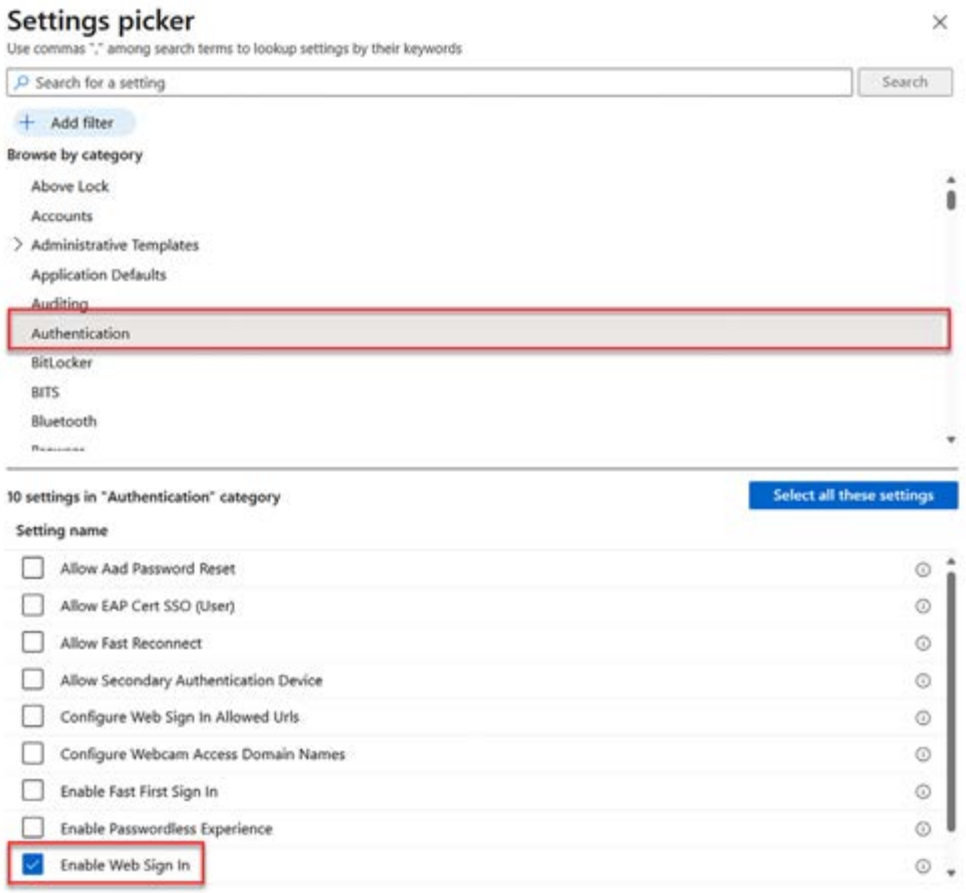


Figure 13.49: Intune authentication policy

3. After enabling it, you will see the web sign-in icon at the logon UI of Windows 11.

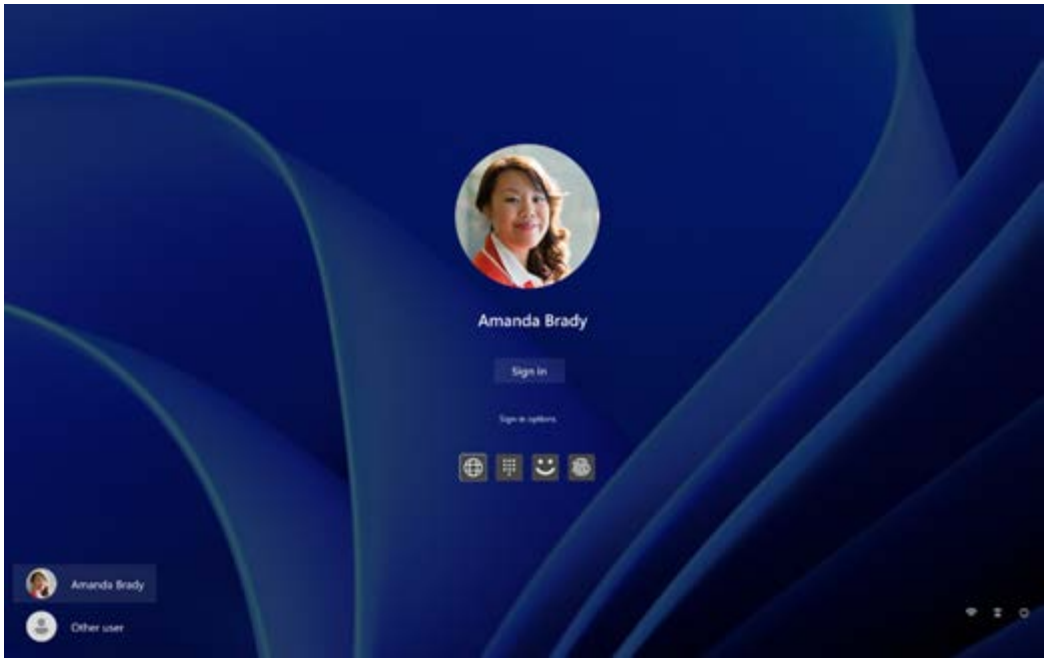


Figure 13.50: Web sign-in Windows UI

BitLocker disk encryption

BitLocker has been available since the first release of Windows Vista and gives the option to encrypt the drives attached to the endpoint. In most cases, BitLocker can work in conjunction with your endpoint that has a **Trusted Platform Module** (**TPM**) chip.

When your end users authenticate to their devices on a day-to-day basis, they will not be asked for the recovery key. But if you are moving the OS disk out of the endpoint and exchanging it for another device or getting a firmware upgrade, you might be asked for the BitLocker recovery key that is associated with your device disk to decrypt everything.

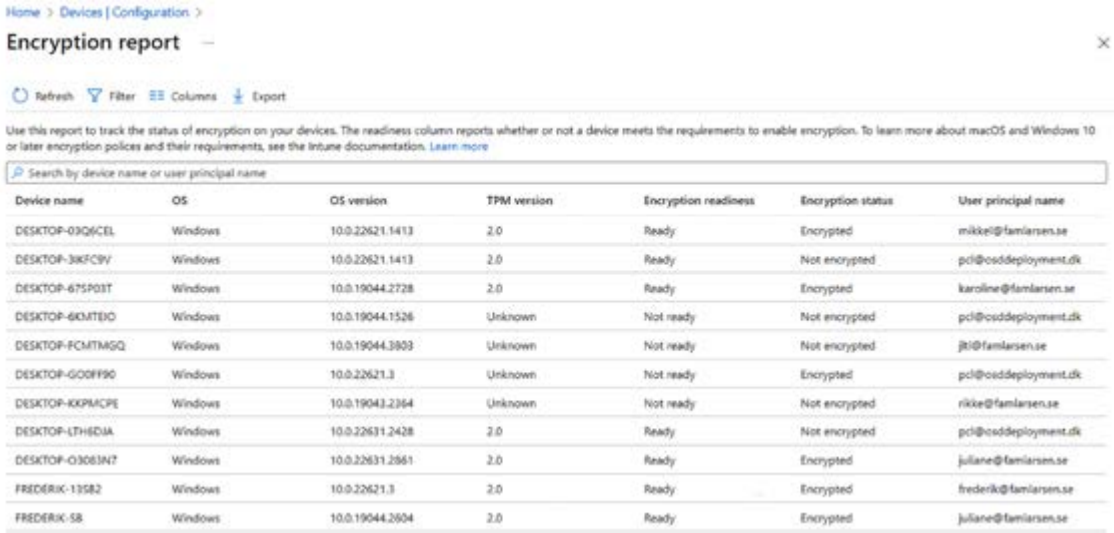


Be aware that BitLocker keys are stored on the Entra device object and not on the Intune device object. If the Entra device object is deleted, it is not possible to retrieve the recovery key again.

We covered in *Chapter 7* how to configure BitLocker when doing Autopilot provisioning – it is no different from the way you need to do it when the device is up and running.

So, here, we will cover the admin task you have on BitLocker management as an IT administrator.

You will have access to the encryption report in Intune from **Devices | Configuration | Encryption report**.



Device name	OS	OS version	TPM version	Encryption readiness	Encryption status	User principal name
DESKTOP-03Q6CEL	Windows	10.0.22621.1413	2.0	Ready	Encrypted	mikkel@famlarsen.se
DESKTOP-3IKFC9V	Windows	10.0.22621.1413	2.0	Ready	Not encrypted	pcl@osddeployment.dk
DESKTOP-675P03T	Windows	10.0.19044.2728	2.0	Ready	Encrypted	karoline@famlarsen.se
DESKTOP-6KMTEJO	Windows	10.0.19044.1526	Unknown	Not ready	Not encrypted	pcl@osddeployment.dk
DESKTOP-FCMTMGQ	Windows	10.0.19044.3803	Unknown	Not ready	Not encrypted	jkl@famlarsen.se
DESKTOP-GO0FF90	Windows	10.0.22621.3	Unknown	Not ready	Encrypted	pcl@osddeployment.dk
DESKTOP-KKPMCPE	Windows	10.0.19043.2364	Unknown	Not ready	Not encrypted	rikke@famlarsen.se
DESKTOP-LTH6DIA	Windows	10.0.22631.2428	2.0	Ready	Not encrypted	pcl@osddeployment.dk
DESKTOP-O3083N7	Windows	10.0.22631.2861	2.0	Ready	Encrypted	juliane@famlarsen.se
FREDERIK-13SB2	Windows	10.0.22621.3	2.0	Ready	Encrypted	frederik@famlarsen.se
FREDERIK-SB	Windows	10.0.19044.2604	2.0	Ready	Encrypted	juliane@famlarsen.se

Figure 13.51: Intune Encryption report

The report will provide you with the details you need to start troubleshooting BitLocker issues on your devices.

BitLocker recovery keys

When a problem happens with your endpoint and you need to recover your drives, you most likely need your recovery key. Luckily, the BitLocker keys are automatically saved to Microsoft Entra but are visible in Microsoft Intune.

You can find the device's BitLocker recovery keys under **Devices | the user's devices | Recovery keys** in Microsoft Intune:

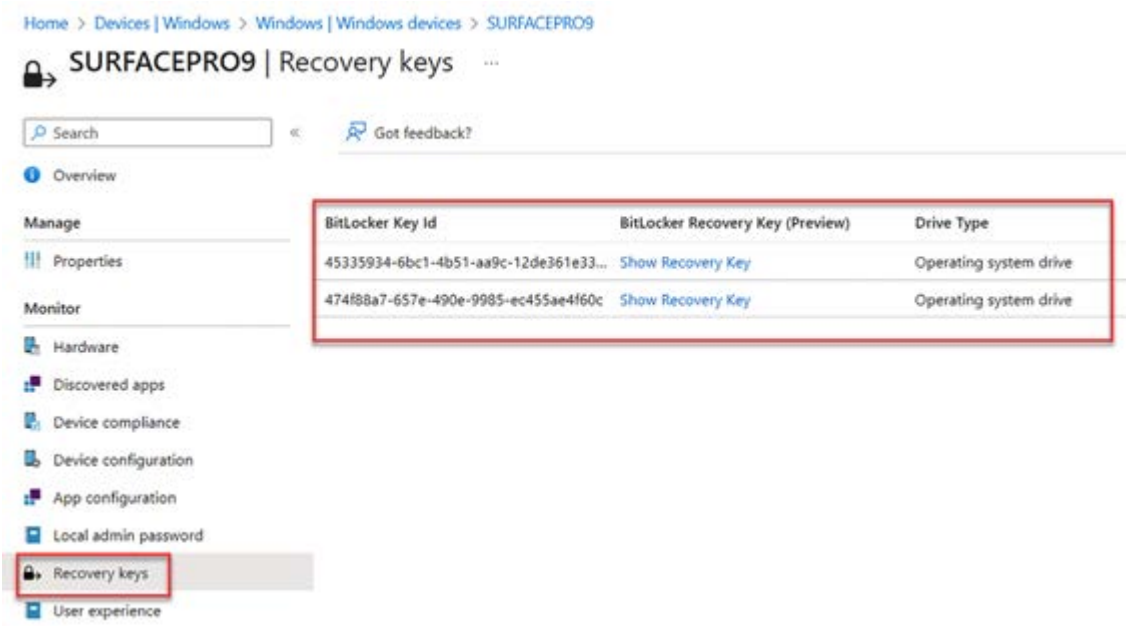


Figure 13.52: BitLocker recovery keys

If you have multiple recovery keys, it is most likely because your device has been reinstalled or the BitLocker keys have been rotated. A BitLocker key will never be deleted on the device object.

If you delete the Intune object for a Microsoft Entra joined device protected by BitLocker, the device deletion will trigger an Intune device sync and will remove the key protectors for the operating system volume.

This will end up in a scenario where BitLocker is in a suspended state on that volume.



BitLocker keys are not stored in Microsoft Intune but on Entra ID. For an IT admin to be able to access the BitLocker recovery key, they need to have `microsoft.directory/bitlockerKeys/key/read in Entra ID`. Some roles in Entra come with that correct permission – Cloud Device Administrator is one example.

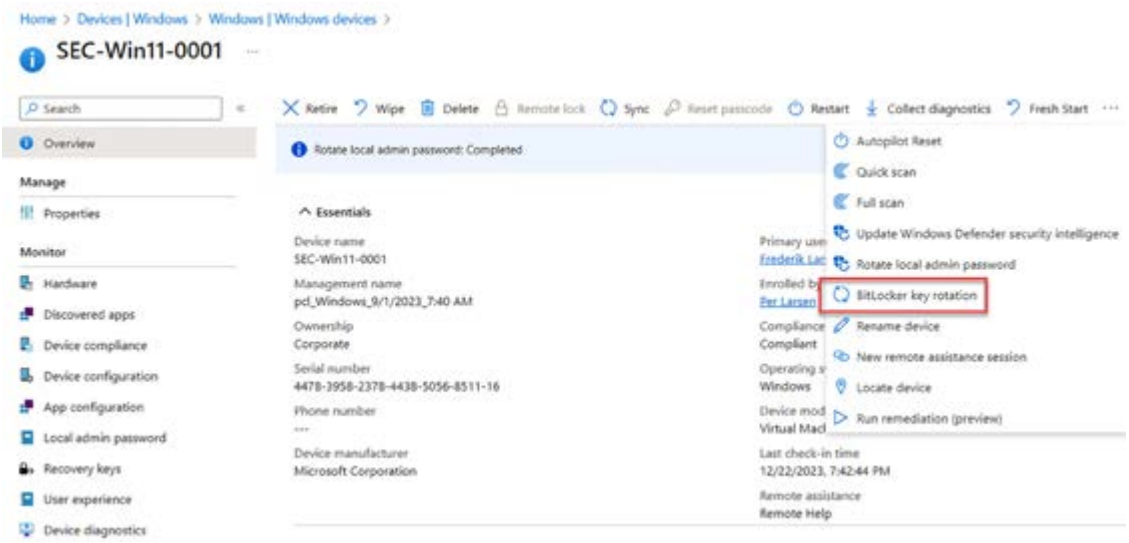


Figure 13.53: BitLocker key rotation

BitLocker key rotation can be triggered from the Intune admin center under Device overview and remote actions.

Enter the recovery key in the key field of the Windows BitLocker recovery wizard and you are good to go!



Figure 13.54: BitLocker recovery

You can search the device's BitLocker recovery keys under **Devices | BitLocker keys** without knowing the device name, in the Entra ID admin center via `https://entra.microsoft.com`.

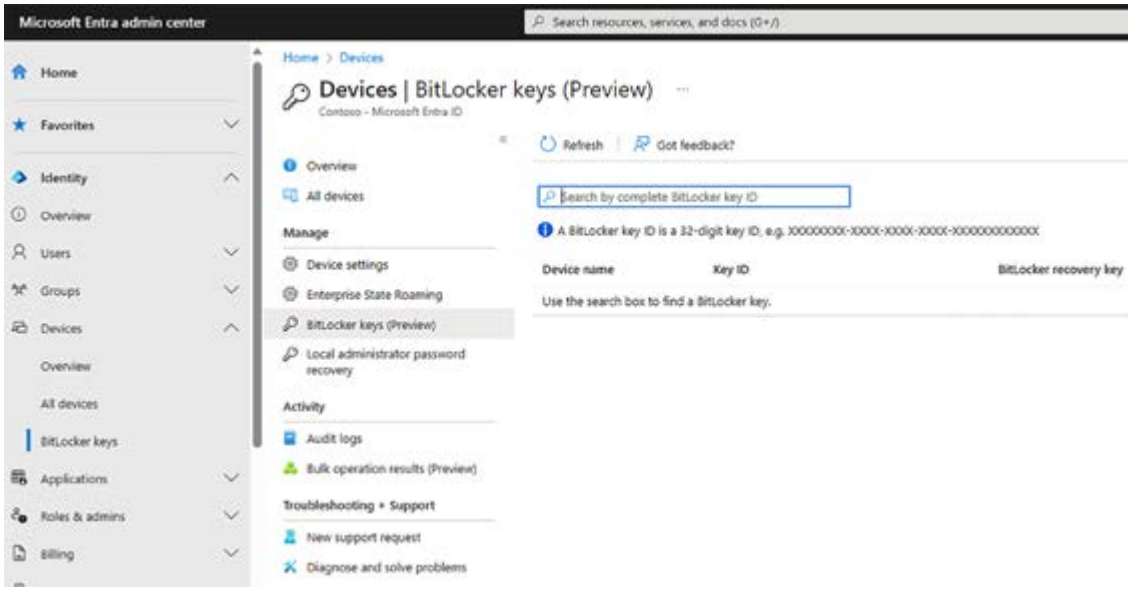


Figure 13.55: Searching for BitLocker keys

Personal Data Encryption

Personal Data Encryption (**PDE**) is a security feature introduced in Windows 11 22H2 that provides file-based data encryption capabilities to Windows. PDE utilizes Windows Hello for Business to link data encryption keys with user credentials. When a user signs in to a device using Windows Hello for Business, decryption keys are released, and encrypted data is accessible to the user. When a user logs off, decryption keys are discarded and data is inaccessible, even if another user signs in to the device. PDE differs from BitLocker in that it encrypts files instead of whole volumes and disks. PDE occurs in addition to other encryption methods, such as BitLocker. To use PDE, the following prerequisites must be met: it must be using Windows 11, version 22H2 and later, and the devices must be Microsoft Entra joined. Domain-joined and Microsoft Entra Hybrid joined devices aren't supported.

Users must sign in using Windows Hello for Business:

1. You can configure it from Microsoft Intune. **Go to Endpoint Security | Disk Encryption | Create Policy**



Figure 13.56: Personal Data Encryption

2. Select the profile Personal Data Encryption.
3. **Enable Personal Data Encryption (User).** Move the toggle to **Enable Personal Data Encryption**
4. Set **Enable PDE on the folder** for the following three options:
    - Protect Pictures (User)
    - Protect Documents (User)
    - Protect Desktop (User)

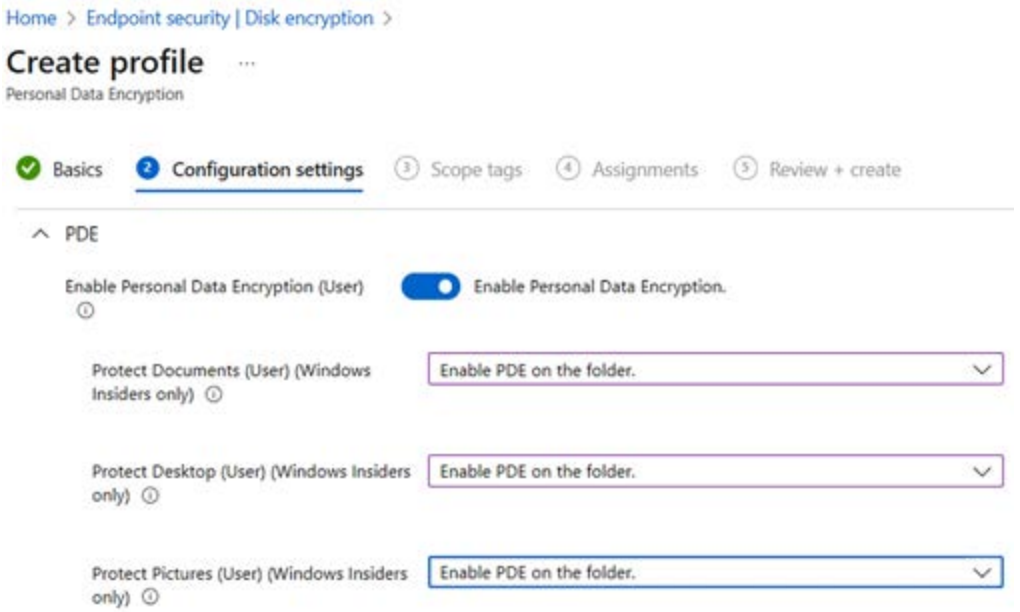


Figure 13.57: Intune PDE policy

You have three options in each folder:

- Disable PDE on the folder. If the folder is currently protected by PDE, this will result in unprotecting the folder.
- Enable PDE on this folder.
- Not configured.

The **Personal Data Encryption** (**PDE**), **Configuration Service Provider** (**CSP**) is used by the enterprise to protect the data confidentiality of PCs and devices. This CSP was added in Windows 11, version 22H2.

Read more in the PDE CSP documentation: `https://learn.microsoft.com/en-us/windows/client-management/mdm/personaldataencryption-csp`.

This is how the sign-in page will look for the end user after enabling PDE.

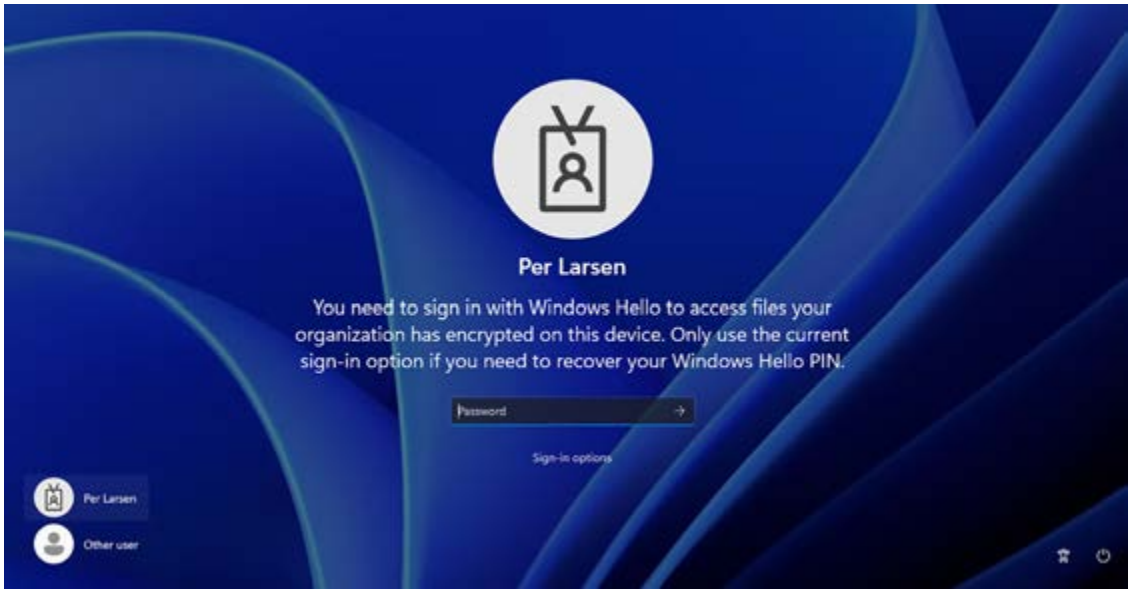


Figure 13.58: PDE Windows sign-in message

This concludes the section on Personal Data Encryption in Microsoft Intune. Next, we will cover the Windows Local Administrator Password Solution.

Windows Local Administrator Password Solution

Windows **Local Administrator Password Solution** (**LAPS**) has different components, such as a Windows, Intune, and Entra component. Windows LAPS can be implemented in a cloud-only environment, where you can manage and back up the password for local administrator accounts. Windows LAPS works on both on-premises AD and Entra. In this book, we will only cover the cloud part of the solution.

Both Windows 10 and 11 are supported but they are required to be updated to the April 2023 cumulative update. Windows LAPS is built into Windows and you do not need to deploy additional binaries to get the Windows LAPS solution working like with the legacy LAPS solution.

Why should you use Windows LAPS?

- It protects against **pass-the-hash** (**PTH**) and lateral moment attacks – as the local password will be unique on each device
- You will be able to sign on a device with a local admin and a password that is only stored on the device in the cloud.
- It works with cloud-only devices and it is built into the management solution when you are using Intune.

First, you need to enable Windows LAPS in Entra:

1. Go to `https://entra.microsoft.com` then **All devices | Device settings**.
2. **Set Enable Microsoft Entra Local Administrator Password Solution (LAPS)** to **Yes** and hit **Save**.

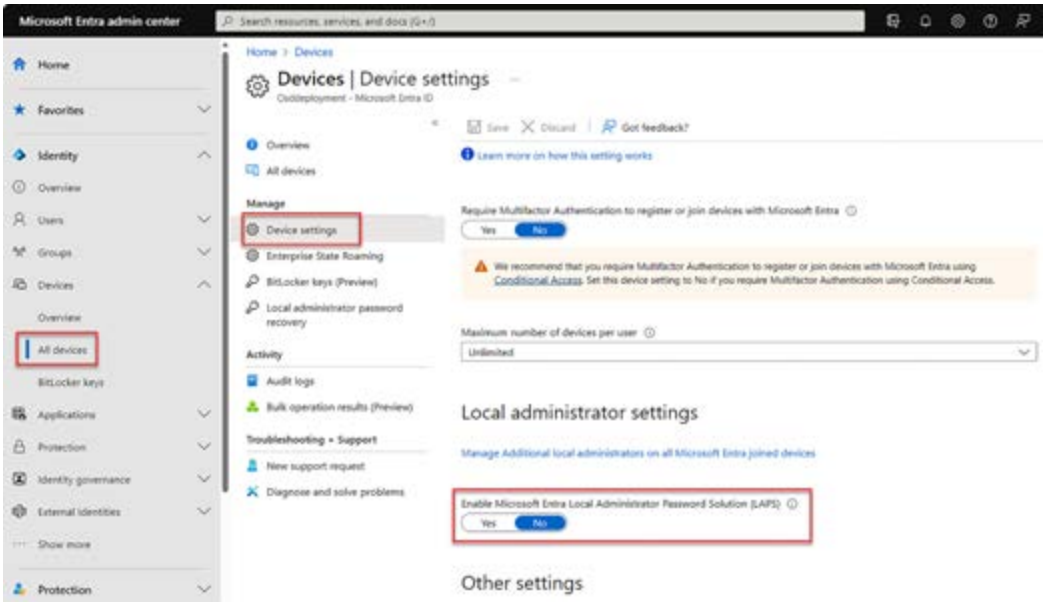


Figure 13.59: Entra LAPS configuration

3. Go to Intune, `https://intune.microsoft.com`, then to **Endpoint security | Account protection.**
4. Click **Create Policy.**

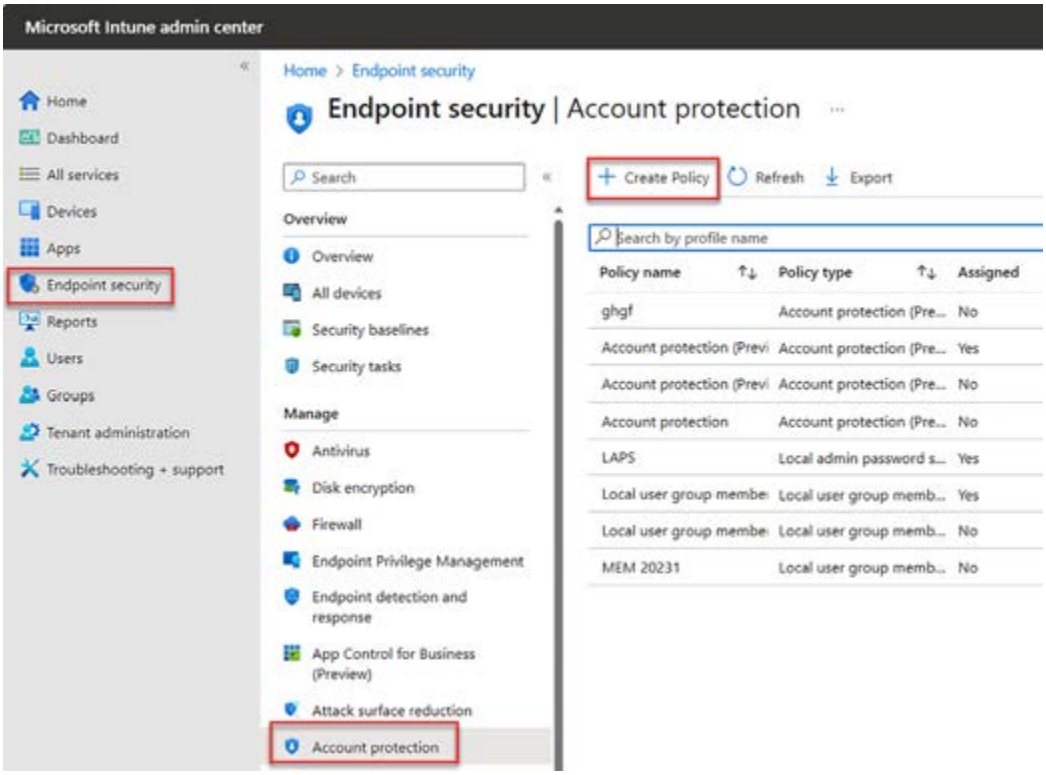


Figure 13.60: Intune Account protection policy

5. Select the platform **Windows 10 and Later.**
6. Select the profile **Local admin password solution (WindowsLAPS).**

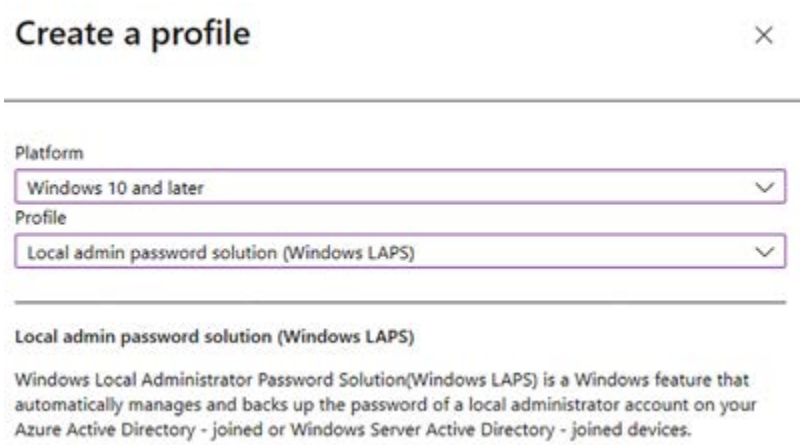


Figure 13.61: Intune Windows LAPS policy

7. Fill out the **Basics** with the policy name, and then move to **Configuration Settings.**
8. Start by choosing the backup directory – **Backup to Azure AD Only.**

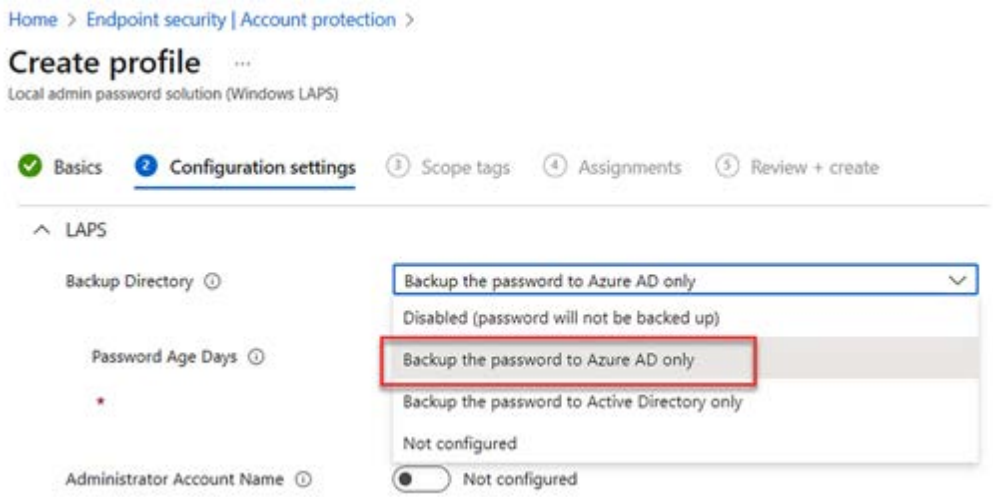


Figure 13.62: Backup to Entra

Configure **Password Age Days.** The default value, if you do not change it, is 30 days. In this case, we will set it to 7 days, so the local admin password will be changed every 7 days on the devices.

We will also rename the local administrator account **Localadmin.**

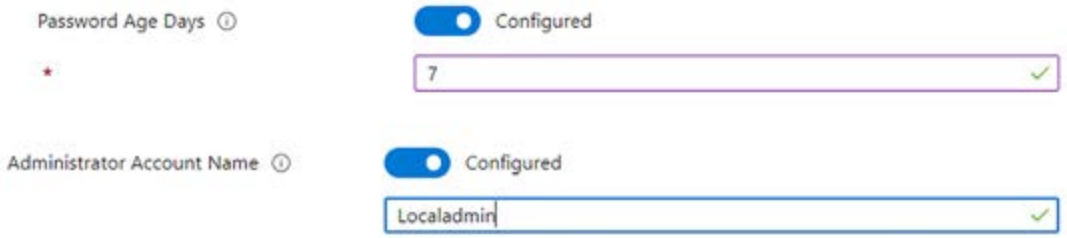


Figure 13.63: Change admin account name

You can set the password complexity. In this case, we are choosing the most complex option.

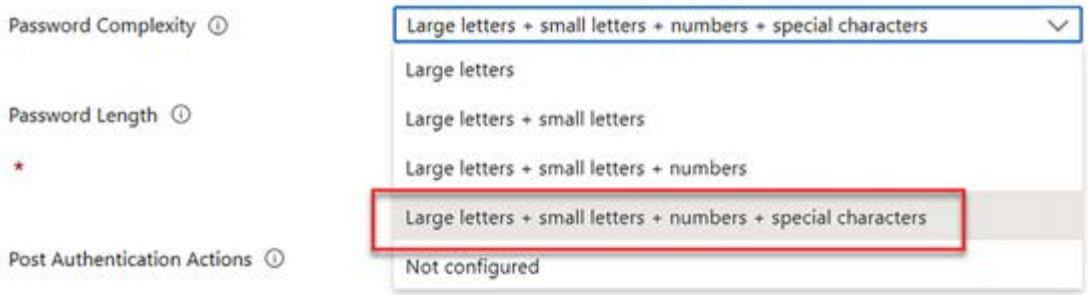


Figure 13.64: Password Complexity

Set the password length to 30 characters. The default value is 14. It cannot be below 8.



Figure 13.65: Password Length

Configuring the post-authentication actions specifies the actions to take upon expiration of the configured grace period.

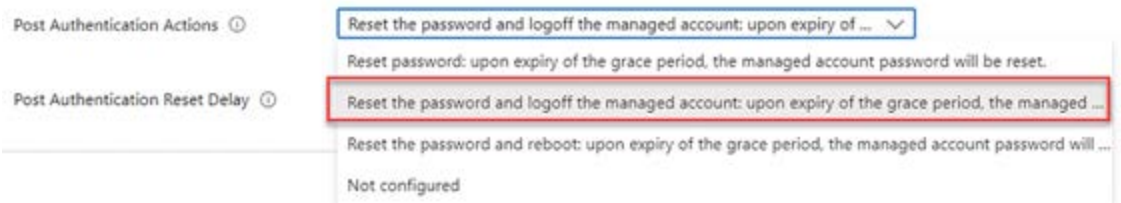


Figure 13.66: Post Authentication Actions

- **Reset password: upon expiry of the grace period, the managed account password will be reset.**
- **Reset the password and logoff the managed account: upon expiry of the grace period, the managed account password will be reset and any interactive logon sessions using the managed account will be terminated.** (Default value if you leave it **Not configured**.)
- **Reset the password and reboot: upon expiry of the grace period, the managed account password will be reset and the managed device will be immediately rebooted.**

Then you just need to deploy the policy to a pilot group to test it.

Read more about the LAPS CSP here: `https://learn.microsoft.com/en-us/windows/client-management/mdm/laps-csp`.

In the Microsoft Intune admin center, you can find the Windows LAPS password under each device.

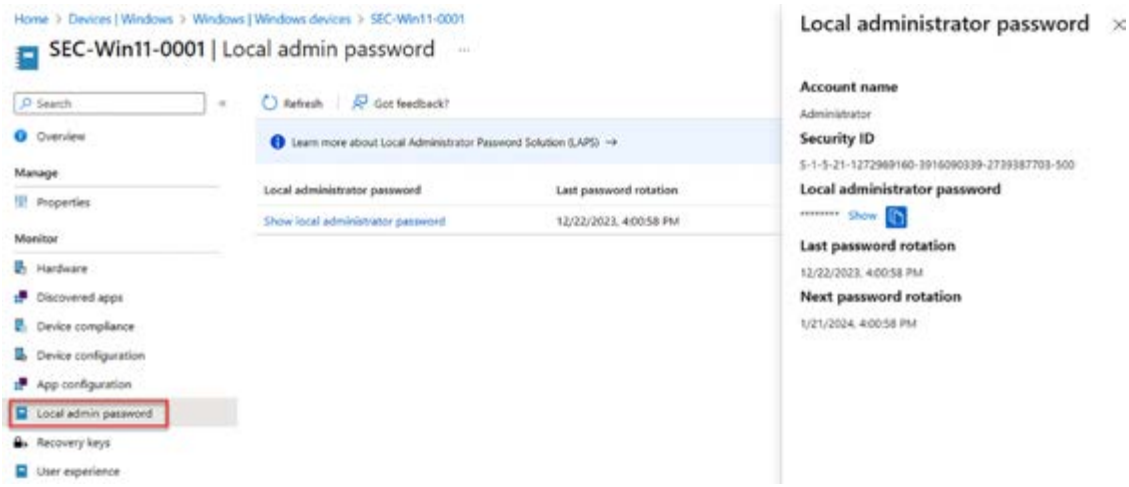


Figure 13.67: Local admin password

As an IT admin, you have the possibility to manually trigger **Rotate local admin password** as a remote action under each device in Intune.

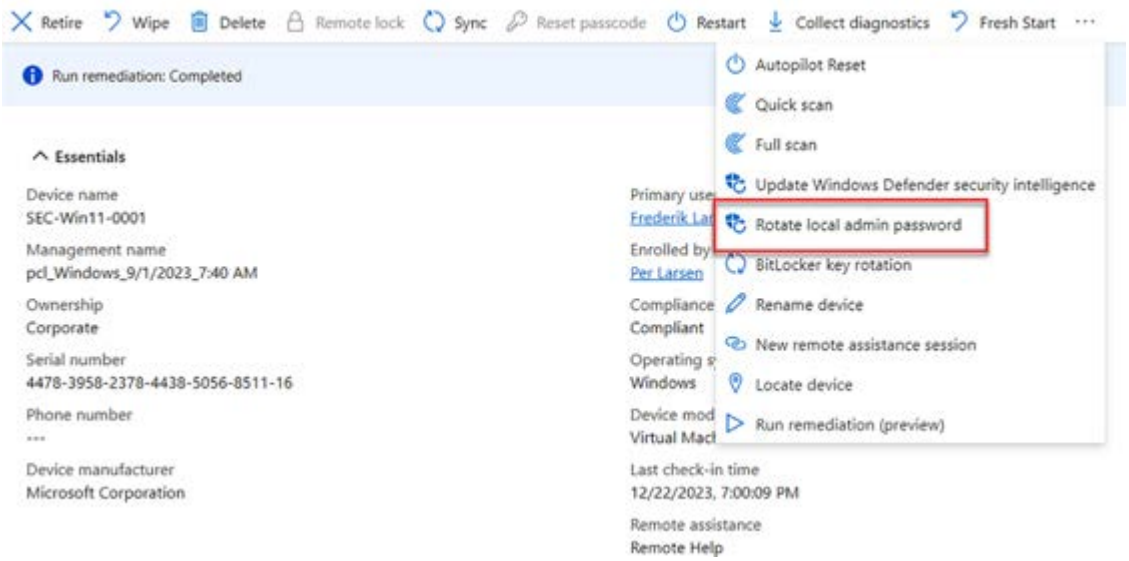


Figure 13.68: Rotate local admin password

It requires a device restart before it takes effect:

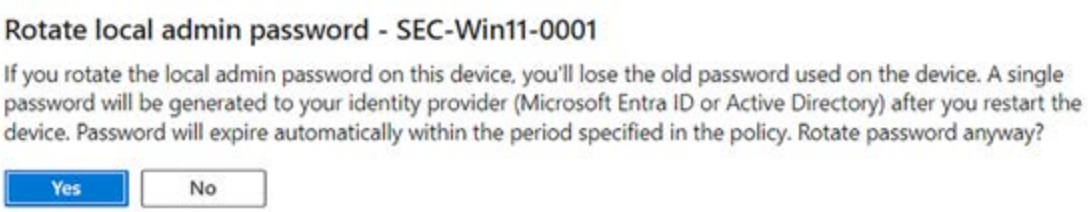


Figure 13.69: Rotate local admin password message

And then it will go back to the normal password rotation specified in the policy.

In the next section, we will look into Application Control for Business, formerly known as **Windows Defender Application Control** (**WDAC**).

Application Control for Business

Application Control for Business is a security feature that blocks or restricts unauthorized drivers and applications from executing in ways that put data at risk. The control functions vary based on the business purpose of the specific application, but the main objective is to help ensure the privacy and security of data used by and transmitted between applications.

Windows 10/11 includes two different technologies that can be used for application control.

One is AppLocker, which we will not cover in this book; we will just say that AppLocker will continue to receive security fixes, but will not get any new feature improvements.

Application Control for Business can be deployed in several different ways, but in this book, we will cover how to use it as follows:

- Managed installer with Intune
- Leverage Microsoft **Intelligent Security Graph** (**ISG**)
- Use Application Control for Business to block certain files

The managed installer within Intune was released in preview in mid-2023.

The big benefit of setting Intune as a managed installer for Application Control for Business is that every app that is being installed from the Win32 app model in Intune will have the managed installer flag set and be allowed to run on your devices. This will minimize the IT admin workload that can come with application control.

The managed installer is also applicable to Windows Pro editions. This means when you go through the Autopilot process with a brand-new Autopilot device shipped directly from the OEM with a Windows Pro image preinstalled, the managed installer will be active as part of that process for all Win32 apps deployed to those devices.

What do you need to know before starting with the managed installer?

- Setting Intune as a managed installer is a tenant-wide configuration, so all devices will be targeted by the policy when you enable it.
- Once devices have the managed installer policy in place, all apps you deploy to Windows devices within the Win32 app model will be tagged.
- This tag in itself has no effect on which apps can run on your devices.
- All existent apps on your devices are not tagged and it only happens on installation after the policy applies to the device.
- You can turn off this policy by editing the managed installer policy.
- Apps that were previously installed while the managed installer policy was active will remain tagged.



Be aware that when the managed installer is in enforce mode, apps will not be able to automatically update themself as you have only allowed Intune as the managed installer and not all the auto-update components from each application.

Let's get started by enabling Intune as a managed installer:

1. Go to the Intune admin center, then to **Endpoint Security | App Control for Business (Preview) | Managed installer.**

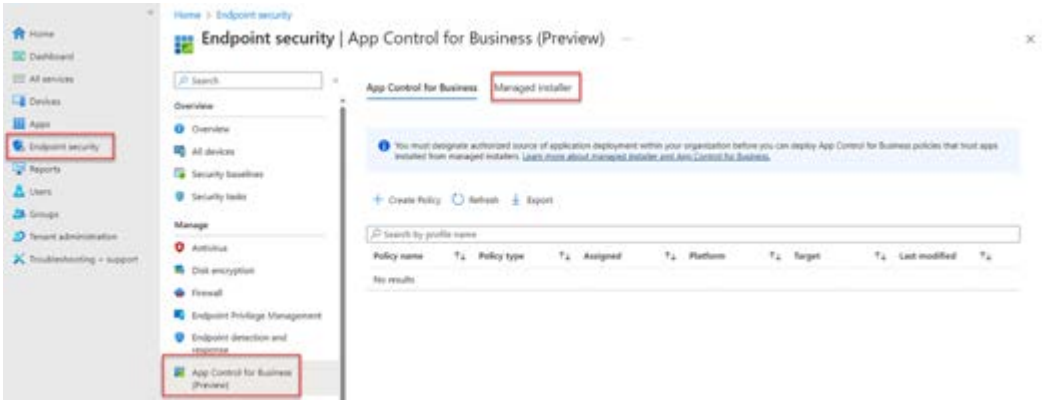


Figure 13.70: App Control for Business managed installer

2. Click **Add**.

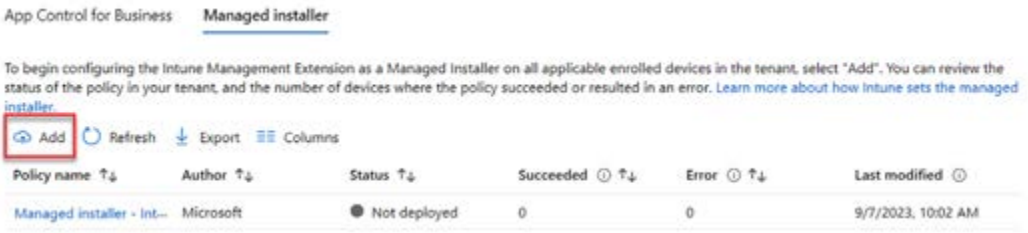


Figure 13.71: Managed installer | Add

You need to read the instructions, and understand that when you click **Add**, the managed installer will be deployed to all Windows devices in your tenant.

3. Click **Add** again.

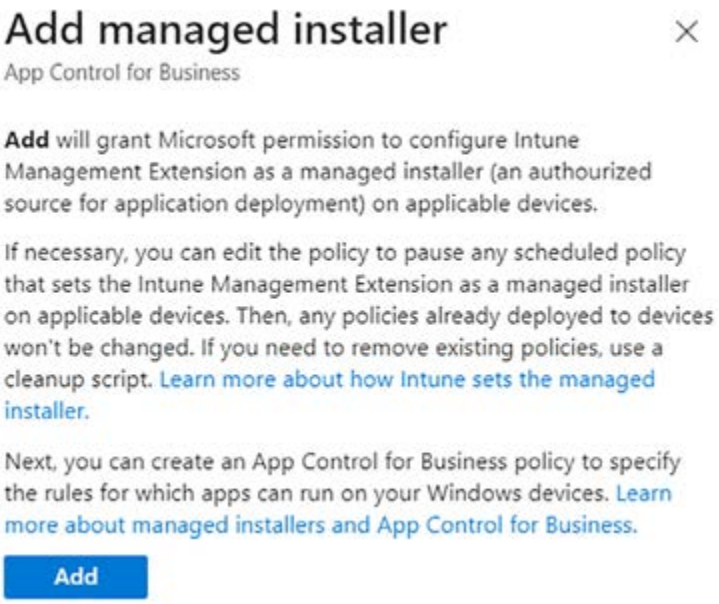


Figure 13.72: App managed installer

4. You need to grant permission to set Intune as a managed installer by clicking **Yes**.

   Then, the managed installer is set to active in your Intune tenant.

5. By clicking on the policy, you can see details on devices that have received the policy.

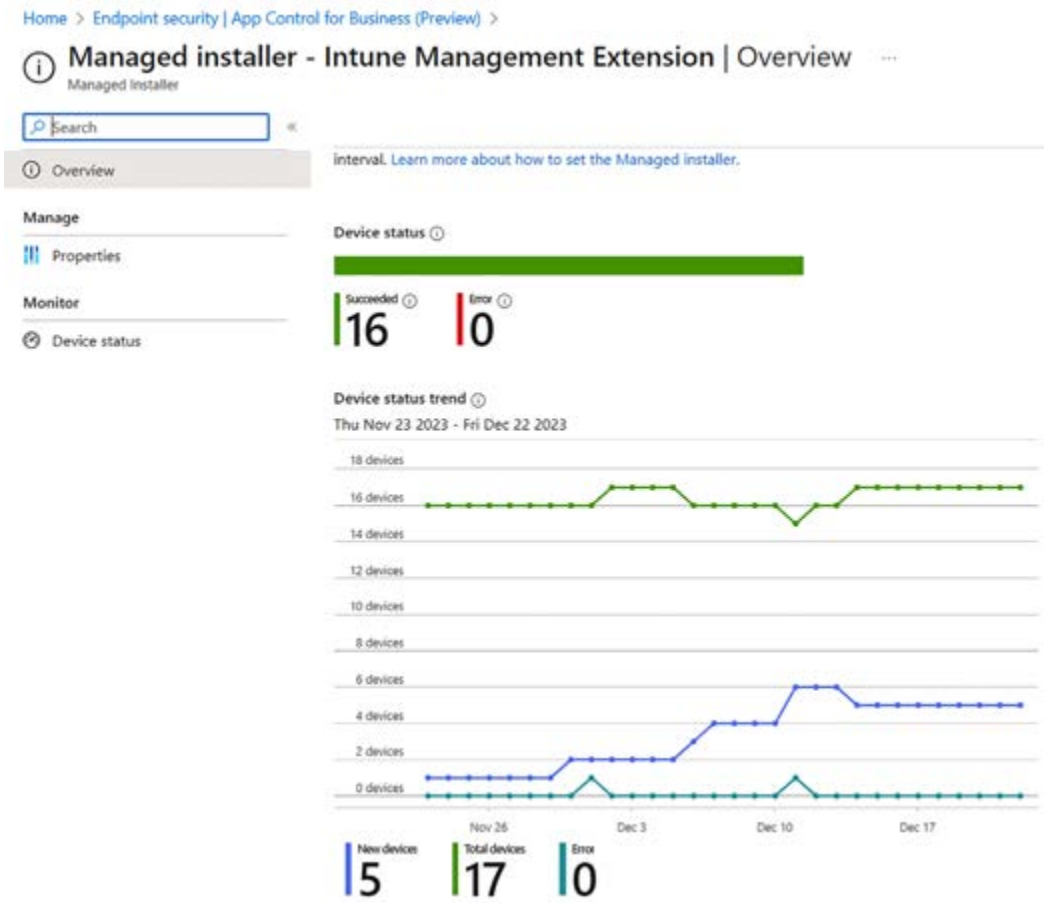


Figure 13.73: Managed installer report

6. If you at a later point want to opt out of the managed installer, you can open the managed installer policy, go to **Properties**, click **Edit** under **Settings**, click **Off** under **Set managed installer**, and hit **Save.**

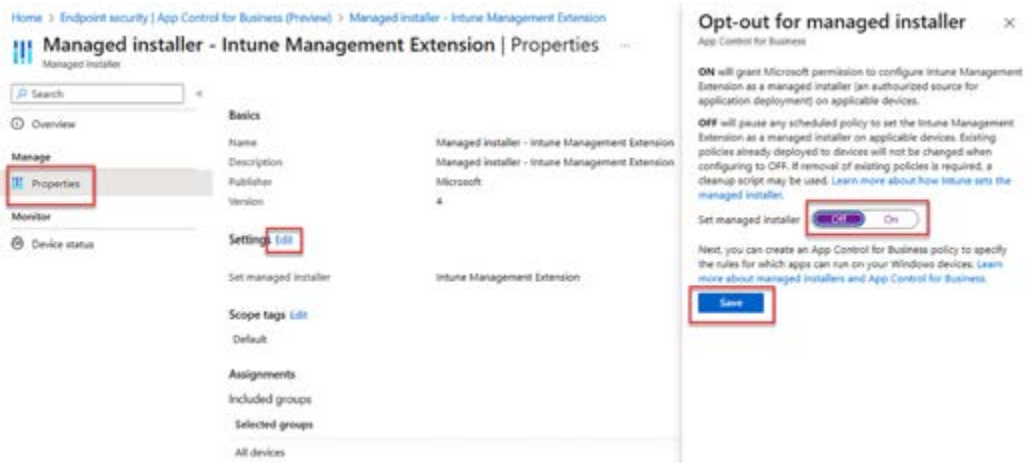


Figure 13.74: Opt-out for managed installer

Then your devices will have the Intune managed installer configuration removed from them.

How does the managed installer get to your devices?

The managed installer leverages Intune remediation scripts to configure the managed installer. Remediation scripts are script packages that consist of a detection script, a remediation script, and metadata. The detection script checks for a specific condition or issue on the device, in this case, if the managed installer is active. If it returns true, it just exits and nothing happens on the device.

The first thing that happens on the device is that a detection script is running on the device:



Figure 13.75: Detect script

If that returns false – it means that Intune is not configured as a managed installer and it will continue to run the remediation script that will set Intune as a managed installer:



Figure 13.76: Remediate script

You can find the details and get to the script by looking at `C:\ProgramData\Microsoft\IntuneManagementExtension\Logs\HealthScripts.log`.

Just search for the managed installer in the log file and you will get the folder where you can find the detect.ps1 and remidate.ps1 that are setting Intune as the managed installer.

If you for some reason need to manually clean up a device, there are a couple of scripts that are helpful.

To remove the Intune management extension as a managed installer from a device, download `CatCleanIMEOnly.ps1` from `https://aka.ms/intune_WDAC/CatCleanIMEOnly`.

To remove all AppLocker policies from a device, download CatCleanAll.ps1 from `https://aka.ms/intune_WDAC/CatCleanAll`.

To see if an application has the managed installer marker, you can leverage `fsutil.exe`.

In this case, we have installed Notepad++ as a Win32 app after onboarding the device into the Intune managed installer.

Run this command:

```
PS C:\Program Files\Notepad++> fsutil.exe file queryEA .\notepad++.exe
```

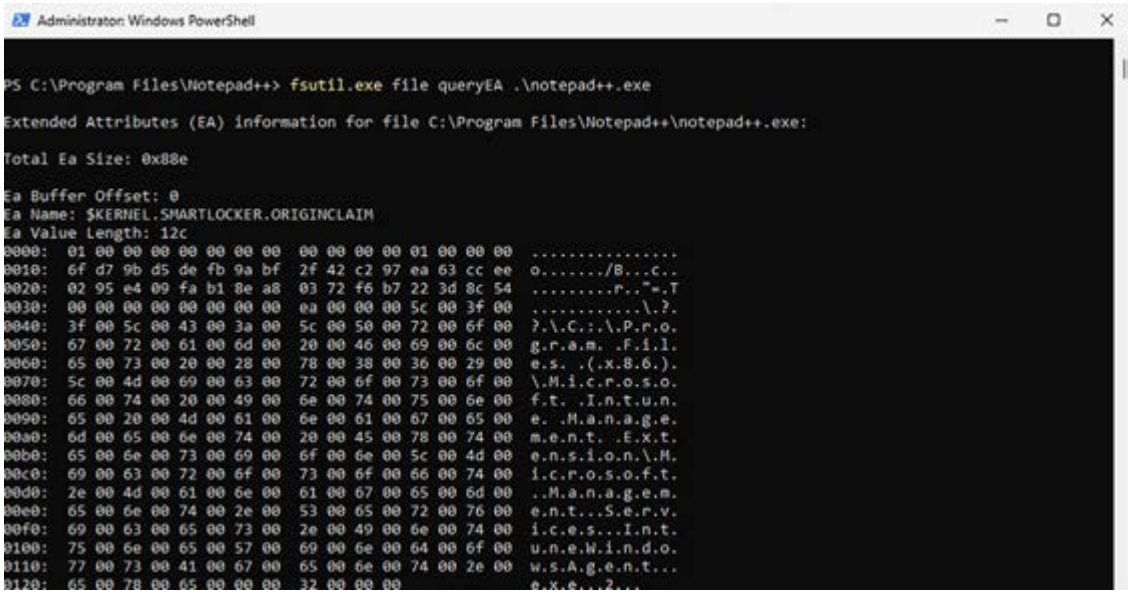


Figure 13.77: queryEA

You can query the **Extended Attributes** (**EAs**) on a file using `fsutil.exe` and looking for the `KERNEL.SMARTLOCKER.ORIGINCLAIM`.

From the first row of data labeled `0000:`, which is then followed by 16 two-character sets. The two-character set will always be `01` as shown here:

```
0000: 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
```

If there is `00` in the fifth position of the output, that indicates the EA is related to the managed installer:

```
0000: 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
```

Finally, the two-character set in the ninth position of the output indicates whether the file was created by a process running as a managed installer. A value of `00` means the file was directly written by a managed installer process and will run if your Application Control for Business policy trusts managed installers.

```
0000: 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
```

If you want to enable Application Control for Business with ISG or put the managed installer in enforce mode on your devices, you need to do the following steps:

1. Go to the Intune admin center and then to **Endpoint Security | App Control for Business (Preview) | Create Policy**.
2. Give the policy a name. Then, click **Next.**
3. Switch **the App Control for Business** policy to **Use built-in controls**.

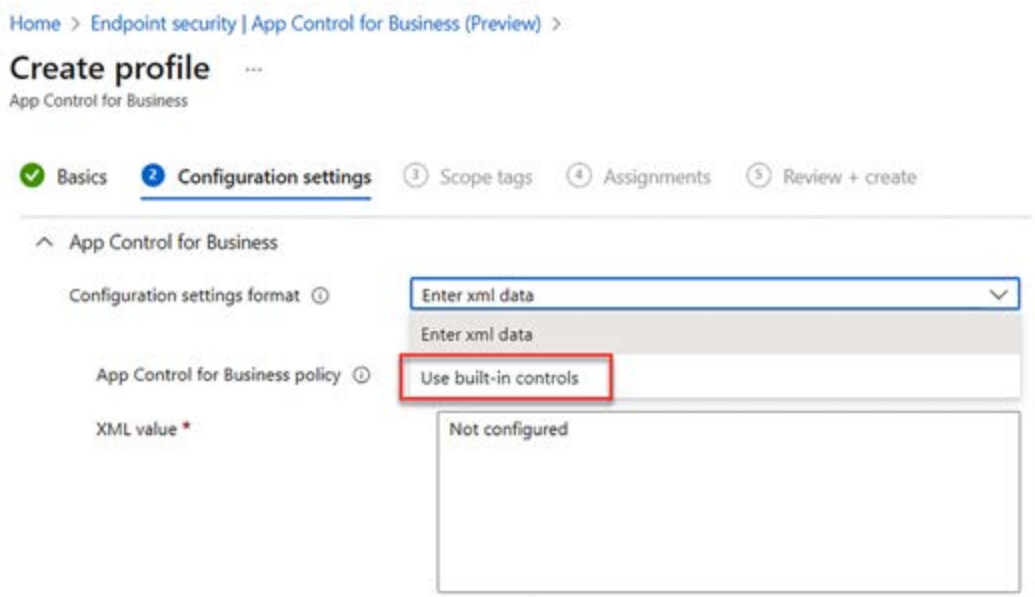


Figure 13.78: App Control built-in controls

4. By setting **Enable App Control for Business policy to Trust Windows components and Store Apps** to **Enforce**, you will trust Windows and App Store apps on your device.
5. Select **Audit only** to log all events in local client logs without blocking any apps from running. Alternatively, choose **Enforce** to actively block apps from running in a deployed App Control for Business base policy.

6. App Control for Business policies created in either **Audit only** or **Enforce** mode will be deployed as rebootless base policies to all targeted devices.

By default, any devices targeted with this App Control for Business policy will have the setting to trust Windows components and Store apps enabled, based on your selection of either audit or enforce mode.

1. Select additional rules for trusting apps.
2. You can leverage both **Trust apps with good reputation** (ISG) and **Trust apps from managed installers**.

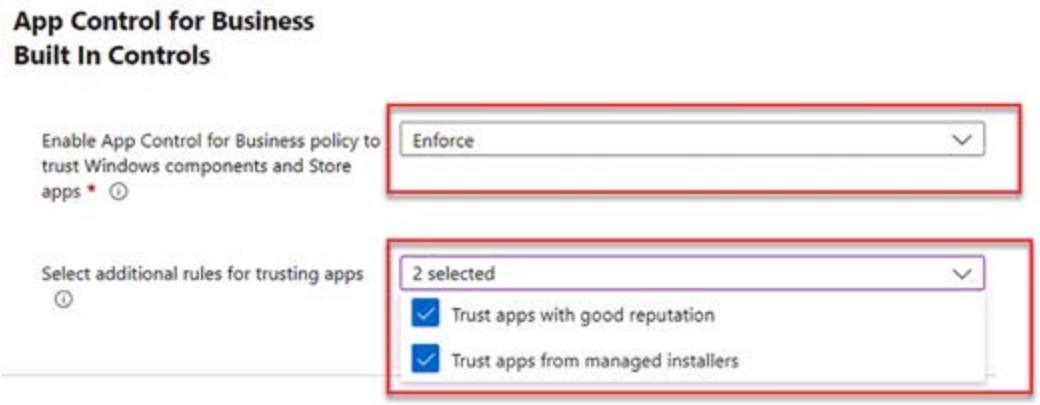


Figure 13.79: Rules for trusting apps

3. Then you just need to deploy it to a test group of devices.

If you want to block apps or just create a custom policy for Application Control for Business, the easy way to do it is by leveraging the Windows Defender App Control Policy Wizard.

You can download the wizard from `https://aka.ms/wdacWizard` as an `.msix` file that you can either install manually or add to Intune as a LOB app and make it available to your fellow IT admins. Every time you start the wizard app, it will check for updates.

We will cover the basic example for creating a policy in this book – but we highly recommend you dig deeper into what you can do with the wizard once you have deployed Application Control for Business in your environment and want to support more complex scenarios:

1. Start **Windows Defender App Control Policy Wizard**.
2. Click **Policy Creator**.

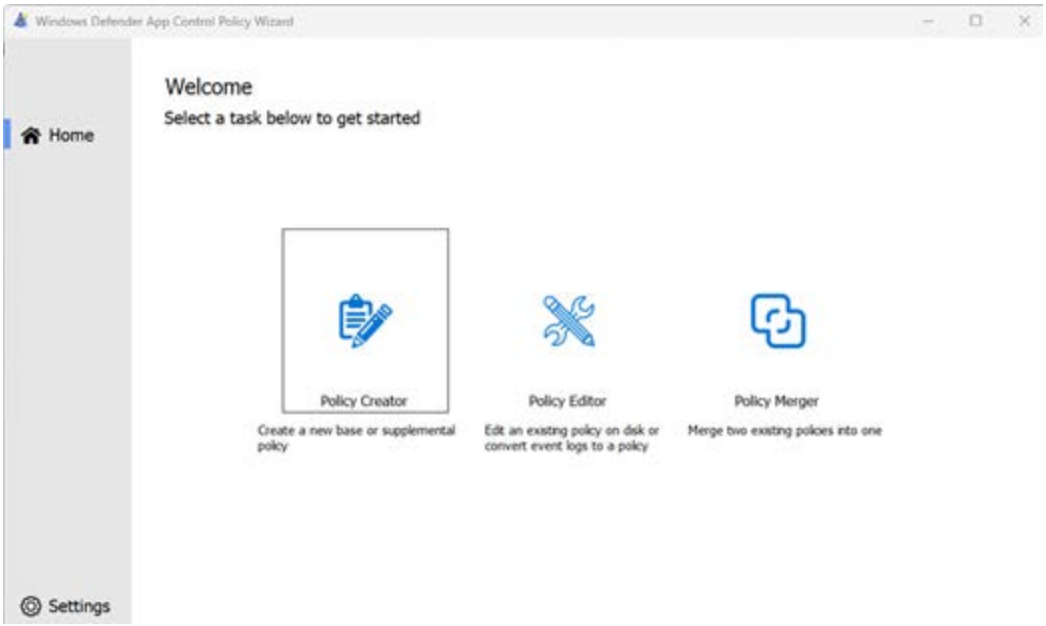


Figure 13.80: Windows Defender App Control Policy Wizard

3. Keep the default to begin with and just click **Next.**

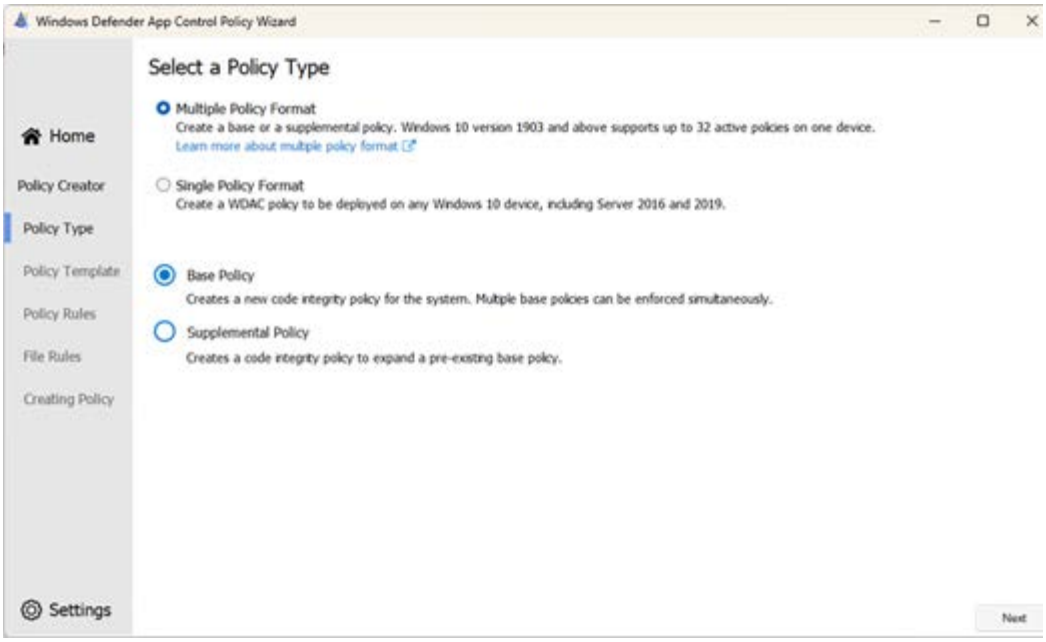


Figure 13.81: Select a policy type

The difference between a base policy and a supplemental policy is that you can add a supplemental policy to a device that already has a base policy applied.

Here are three examples of different use cases (there are many more):

- You have a base policy that covers the entire company, and now you want to make a supplemental policy that only applies to the finance department.
- You have been running Application Control for Business in your environment for a while, and now you need to whitelist some new LOB apps.
- You want to add a block list to the baseline policy you have already deployed.

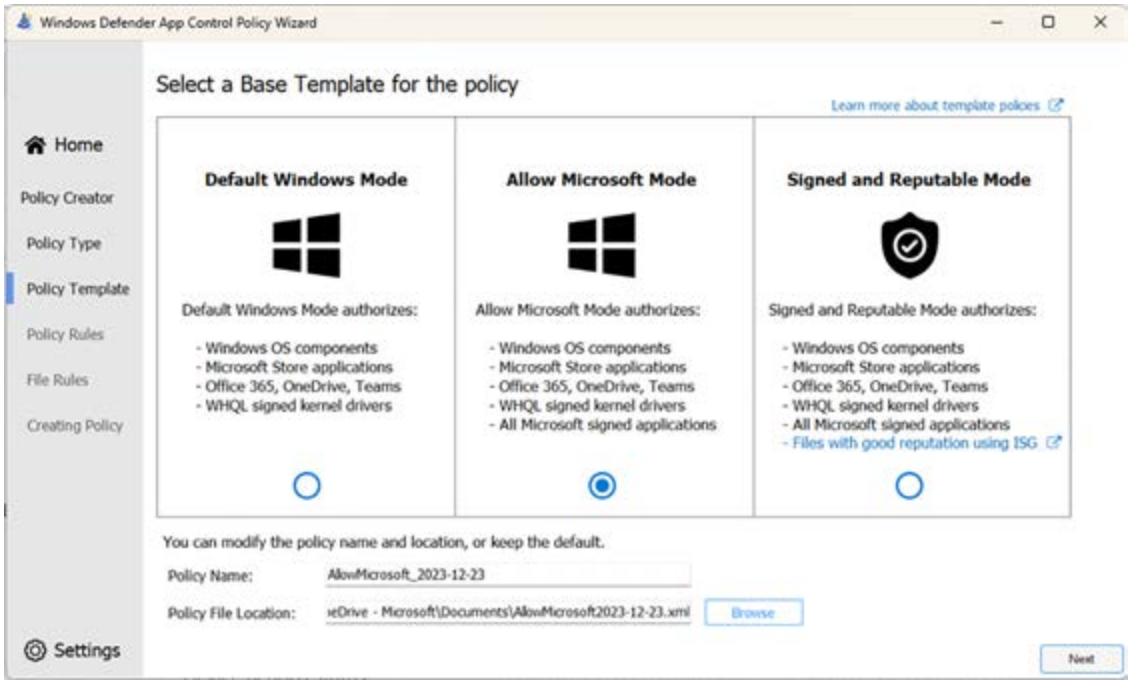


Figure 13.82: Base Template

As you can see, there are three different base templates that you can start leveraging, depending on what you are trying to accomplish. In this case, we will leverage the one in the middle: **Allow Microsoft Mode**.

That will whitelist all Windows OS, Office 365, and WHQL-signed kernel drivers and all Microsoft-signed applications – that is a good start for an office worker's desktop to allow standard apps to run.

1. Then click **Next**.

   All three templates can be found on a Windows Defender App Control Policy Wizard that you have installed in this location: `C:\Windows\schemas\CodeIntegrity\ExamplePolicies`.

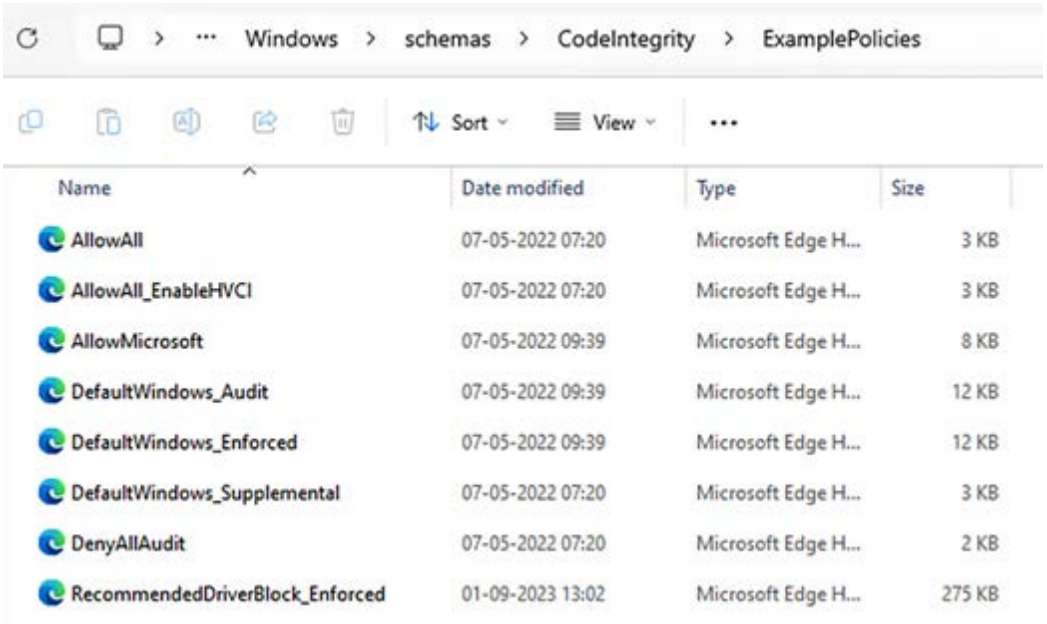


Figure 13.83: Base template on Windows

2. Continue with the wizard.

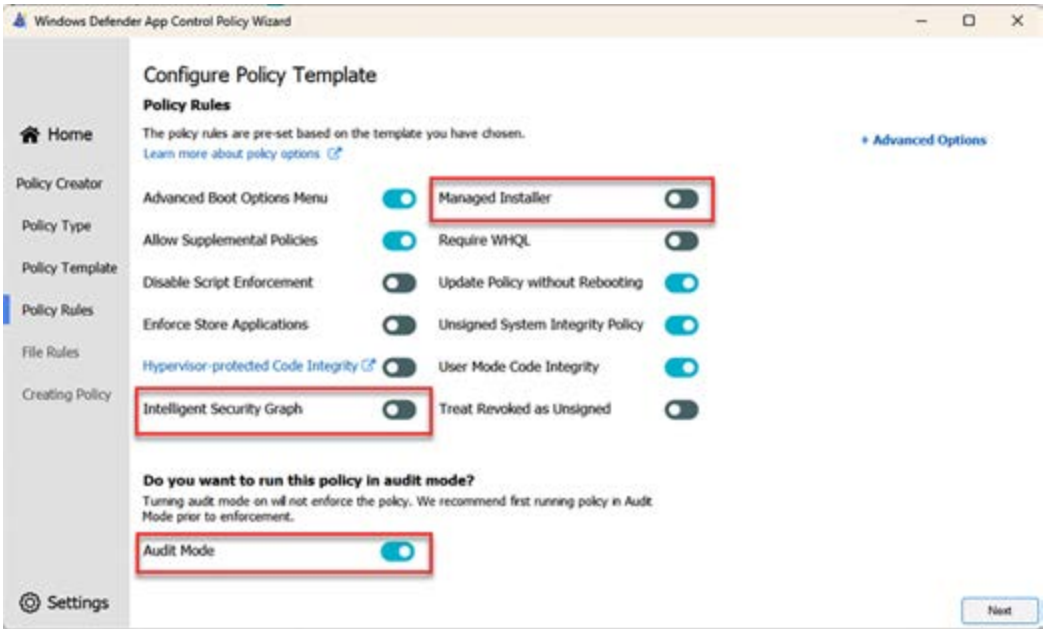


Figure 13.84: Policy Rules

As you can see, you can also leverage the wizard to set Application Control for Business to ISG and managed installer mode. Unless you change Audit Mode in the wizard, that is what you will configure in the `.xml` outcome file at the end of the wizard.

3. Click **Next.**

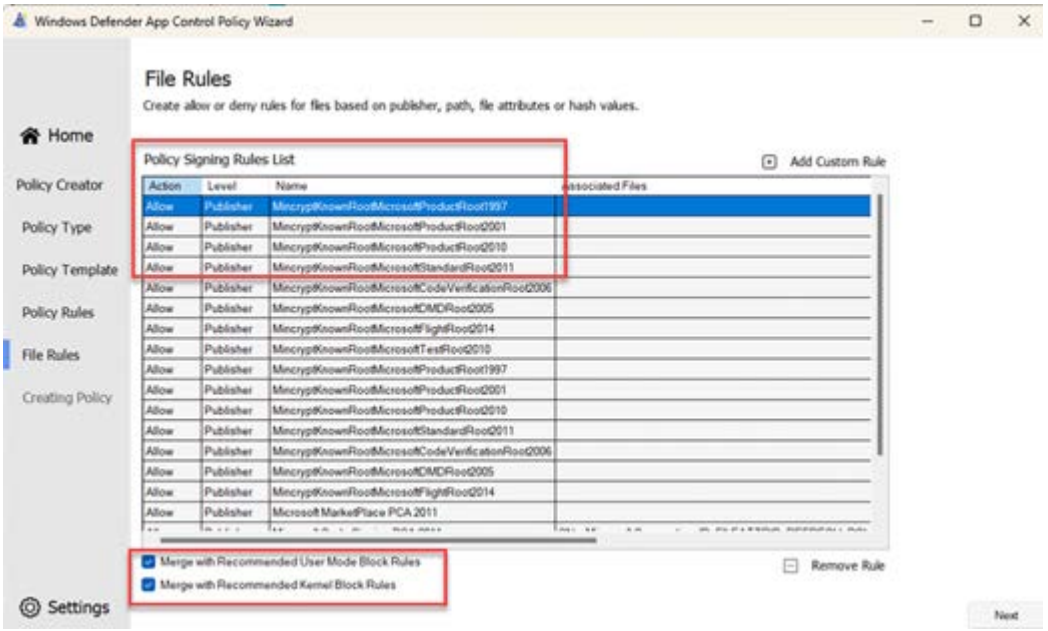


Figure 13.85: Policy Signing Rules List

You can see what allow/deny action has been configured in the policy.

You can also leverage **Merge** options:

- **Merge with Recommended User Mode Block Rules**
- **Merge with Recommended Kernel Block Rules**

We will also suggest you take a look at these two recommendations:

- **Applications that can bypass WDAC and how to block them:** `https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/applications-that-can-bypass-wdac`
- **Microsoft recommended driver block rules:** `https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/microsoft-recommended-driver-block-rules`

Finally, you are at the end of the wizard – and the tool will then build you the policy in the form of an XML file, which you can deploy from Microsoft Intune.

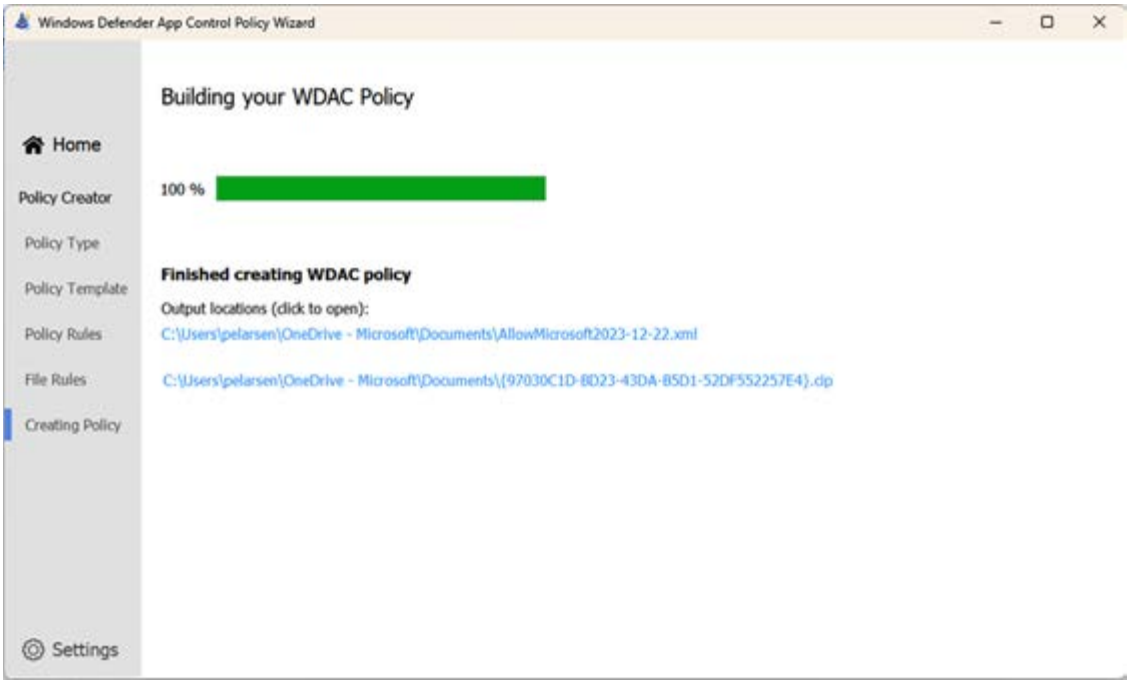


Figure 13.86: Building your WDAC policy

Now we will show you how to create an Application Control for Business policy in Intune with the XML that you just created with the wizard:

1. Go to the Intune admin center and then to **Endpoint security | App Control for Business (Preview) | Create Policy**.

2. Give the policy a name. Then, click **Next**.

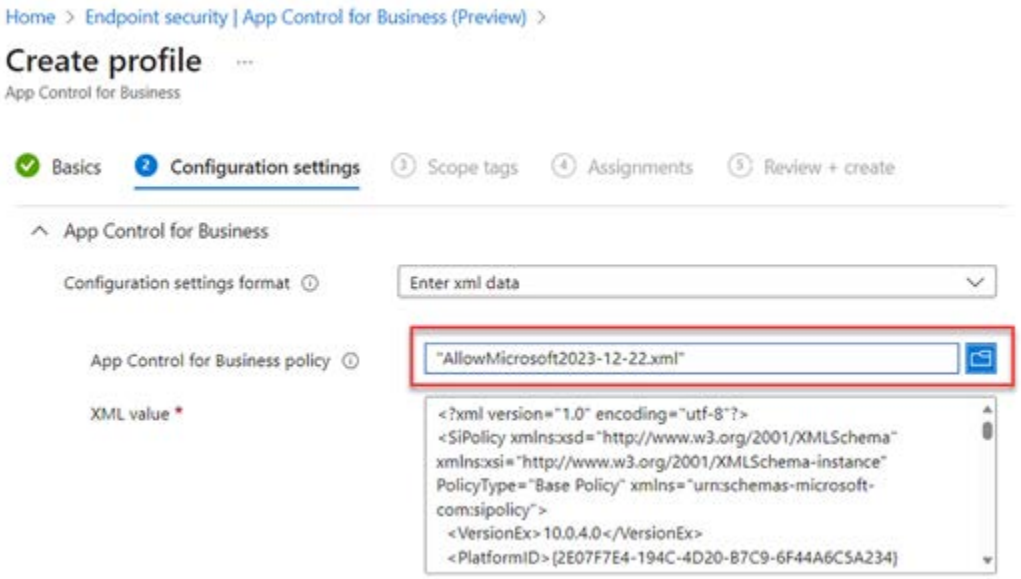


Figure 13.87: App Control for Business policy XML

3. Upload the XML files you just created with the wizard – and then click **Next** until you can assign the policy to a group of test devices.
4. When the policy is applied to the devices and the end user is trying to start an application that is blocked, they will get a message like this:

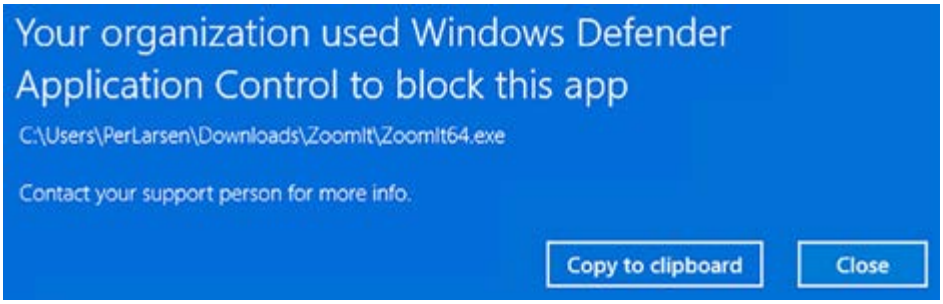


Figure 13.88: App Control end user block notification

This ends the section on Application Control for Business. In the next section, we will go into Defender for Endpoint.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is Microsoft's Enterprise endpoint security platform that was created to help businesses prevent, investigate, detect, and respond to threats. This serves to increase the level of security of your whole endpoint configuration.

Microsoft Defender for Endpoint is a security solution that includes risk-based vulnerability management and assessment, attack surface reduction, behavioral-based and cloud-powered next-generation protection, **endpoint detection and response** (**EDR**), automatic investigation and remediation, managed hunting services, rich APIs, and unified security management.

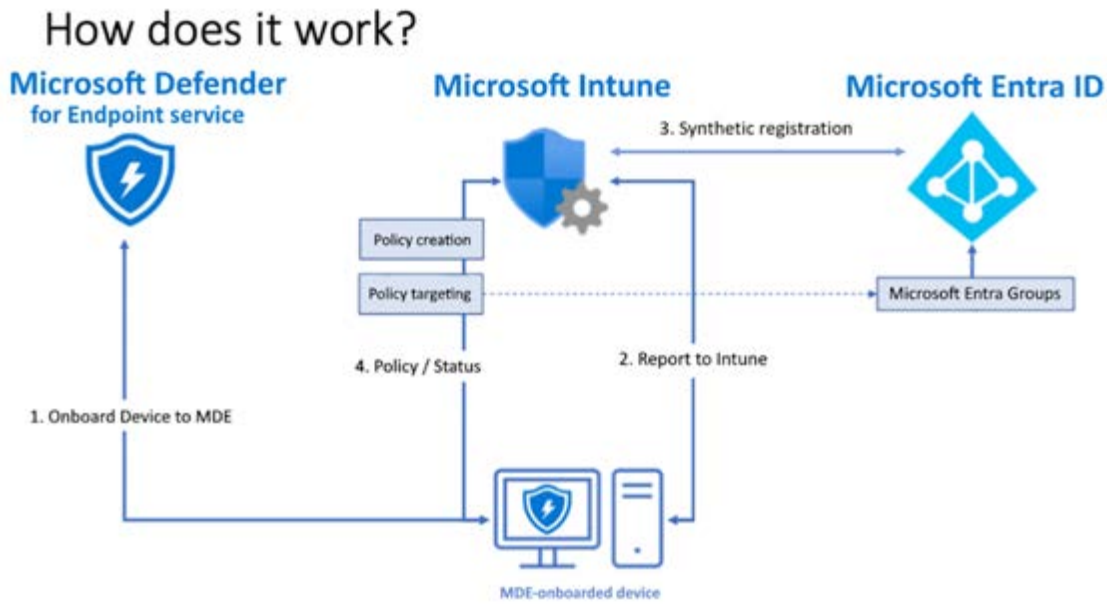


Figure 13.89: Microsoft Defender for Endpoint service architecture

Integration with Microsoft Intune

Microsoft Intune is becoming more and more prominent for customers who are using Windows 365/Azure Virtual Desktop as it provides a unified way of configuring and maintaining your physical and virtual cloud endpoint as well as other devices, such as mobile.

Microsoft Defender for Endpoint integrates seamlessly into Microsoft Intune. You only need to activate the Intune integration once during the initial setup and your reports will flow into Microsoft Intune.

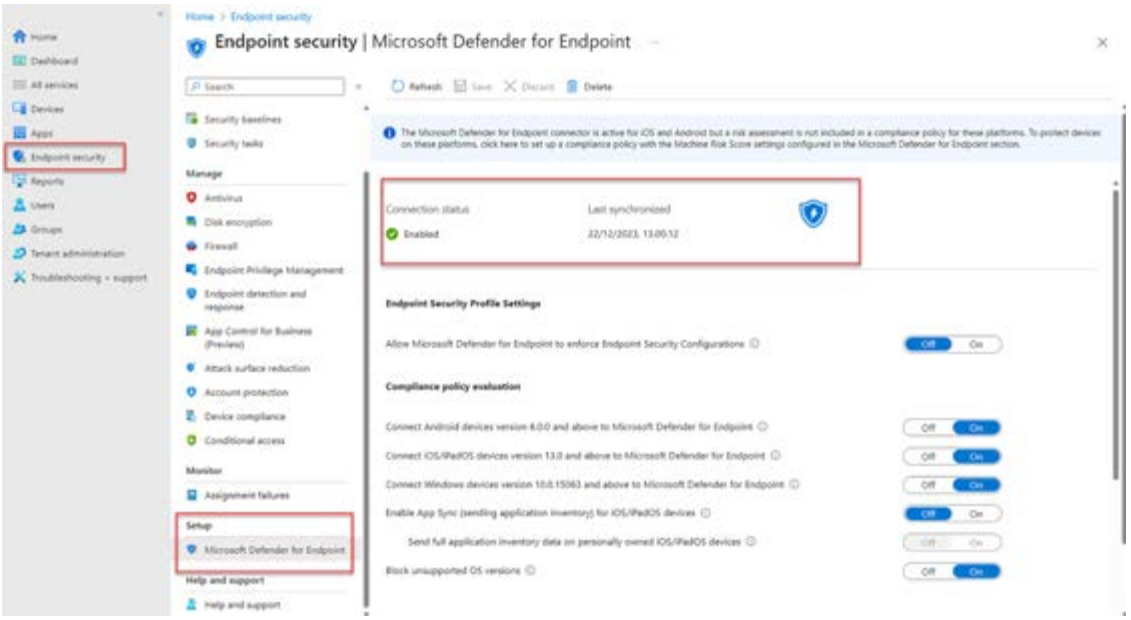


Figure 13.90: Microsoft Defender for Endpoint

This concludes the overview of Microsoft Defender for Endpoint. Next, we will give you an overview of the security baselines.

Security baselines

Security baselines are preconfigured groups of Windows settings that help you apply the security settings that are recommended by the relevant security teams. The baselines you deploy can be customized to enforce only the settings and values required by you.

There are multiple security-related settings in Windows as well as for Microsoft Edge for your endpoints. Another great asset is the option to do versioning and filtering based on different OSes or scenarios that have to be stricter. You no longer have to use GPOs to ensure the security settings on your endpoints – just create a security baseline profile and you're all set.

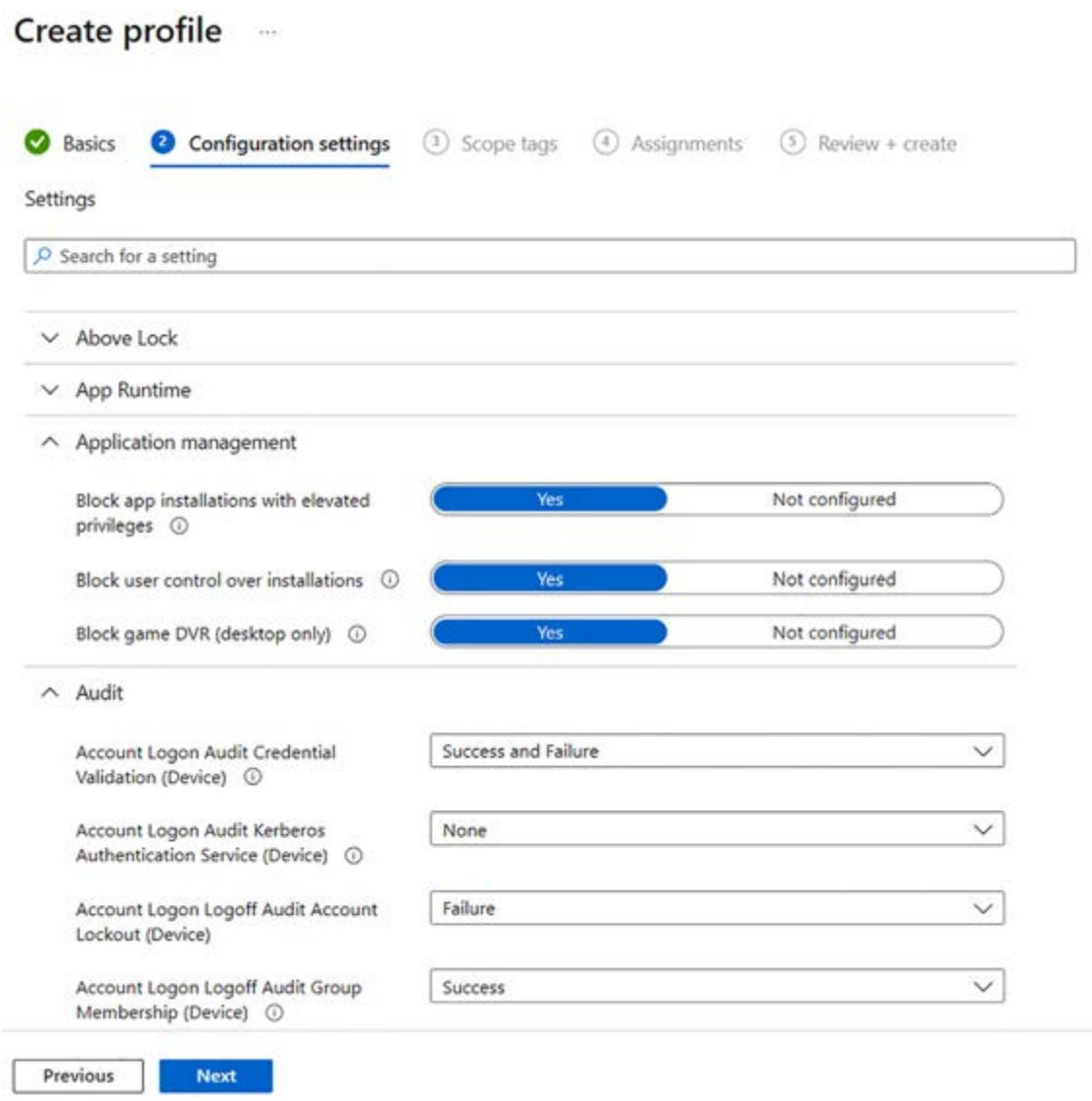


Figure 13.91: MDM security baselines

This concludes this security baseline overview. Next, we will cover compliance policies.

Compliance policies

We can define the rules and settings that users and devices must meet to be compliant. This can include actions that apply to non-compliant devices. Actions for noncompliance can alert users to the conditions of noncompliance and safeguard data on non-compliant devices.

See the following example of how you can set the risk level within Microsoft Defender when your endpoint does not meet the compliance expectations. Your device will show up as a risk in Microsoft Defender for Endpoint as well as in Intune – marked as non-compliant.

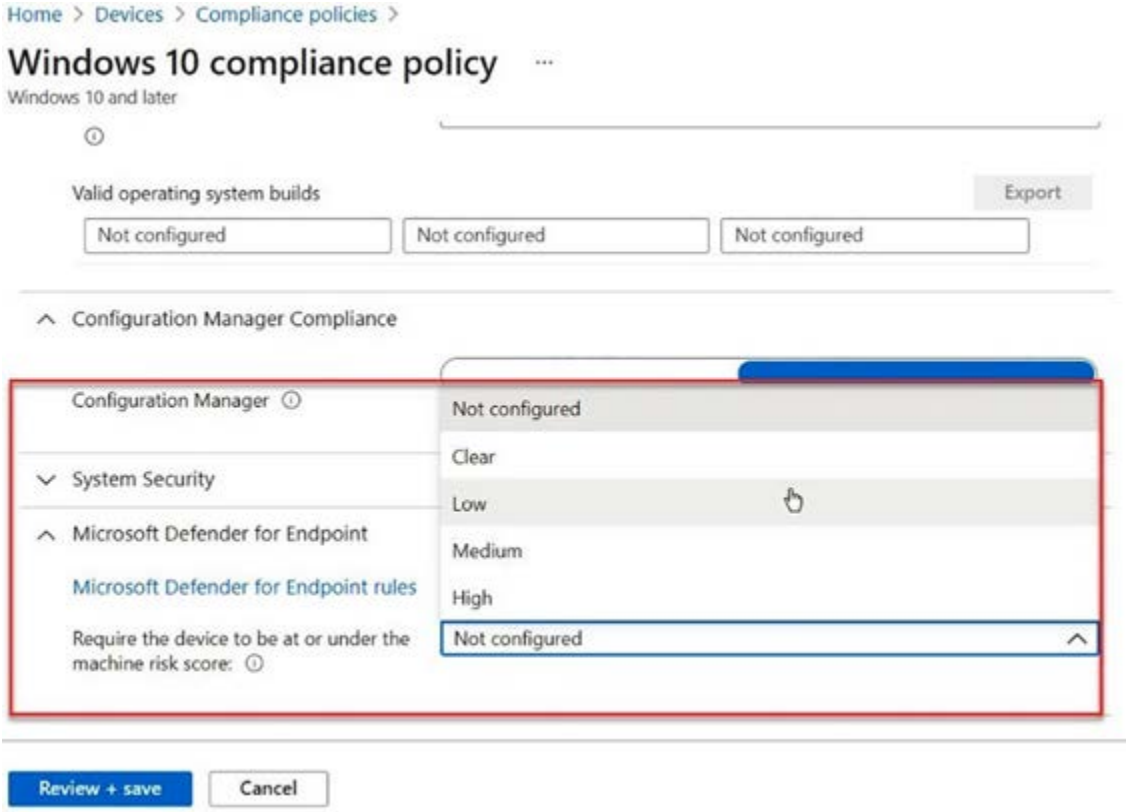


Figure 13.92: Microsoft Defender for Endpoint compliance settings



More information on compliance policies can be found in *Chapter 10*, *Advanced Policy Management*.

Windows 365 security baselines

Windows 365 delivers its own branded set of security baselines that includes different best practices that are optimized for cloud PC virtualized scenarios.

We highly recommend customers use these as they are based on experience from real-world implementations. You can use these policies to lower the risk while increasing the security boundaries of your cloud PCs.

You can use security baselines to get security recommendations that can help lower risk. The Windows 365 baselines enable security configurations for Windows 10, Edge, and Microsoft Defender for Endpoint. They include versioning features and help customers choose when to update user policies to the latest release.



Figure 13.93: Security baselines

This concludes the section on Windows 365 baselines. In the next section, we will cover Defender for Endpoint.

Microsoft Defender for Endpoint

In the next part of this section, we are going to explain how you can configure Microsoft Defender for Endpoint via Microsoft Intune to secure your virtual or physical Windows endpoints:

1. Go to the Microsoft Intune admin center via `https://intune.microsoft.com/#home`.

2. Go to **Endpoint security.**

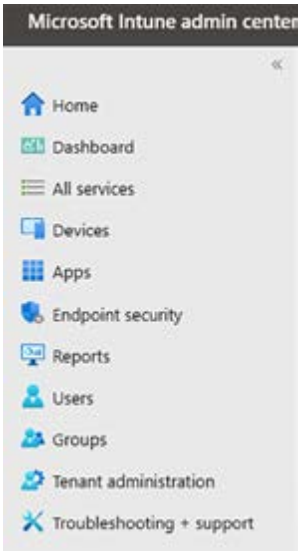


Figure 13.94: Endpoint security

3. Click on **Open the Microsoft Defender Security Center.**

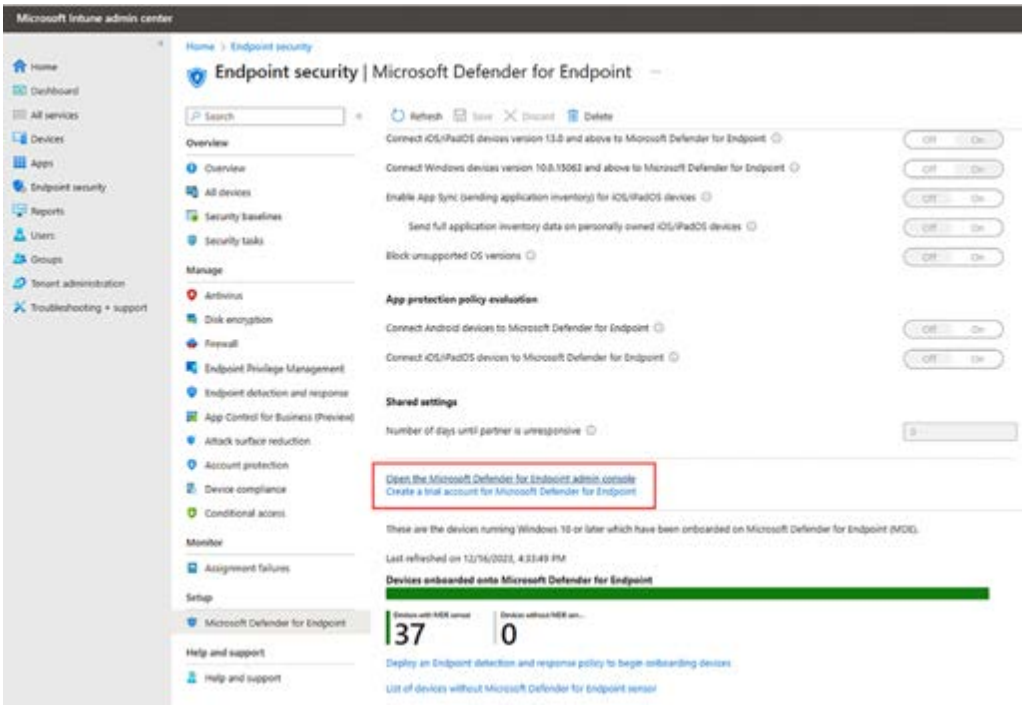


Figure 13.95: Microsoft Defender for Endpoint

4. Click on **Next.**

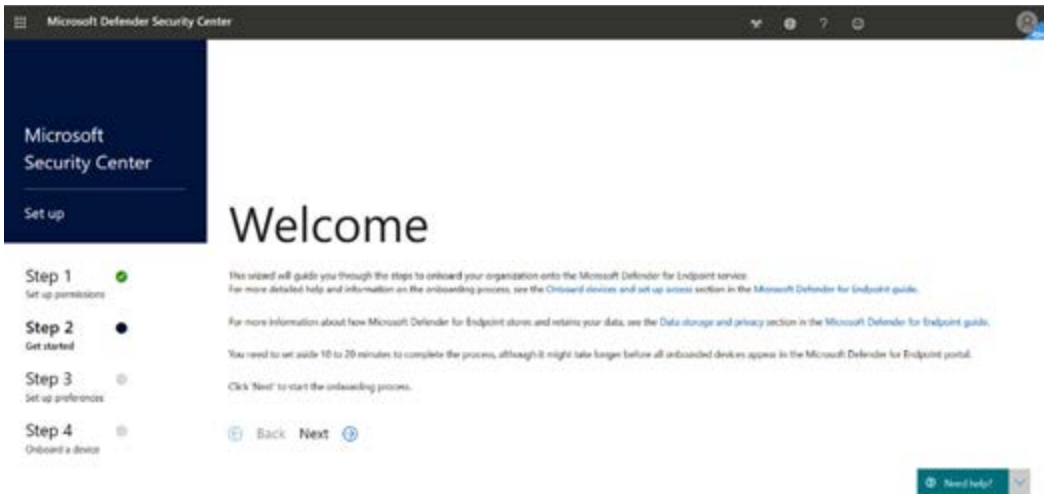


Figure 13.96: Microsoft Defender Security Center – Step 2

5. Fill in your region, data retention policy time, and organization size.



You could also select the **Preview features** option to be among the first to try upcoming features.

6. Click **Next.**

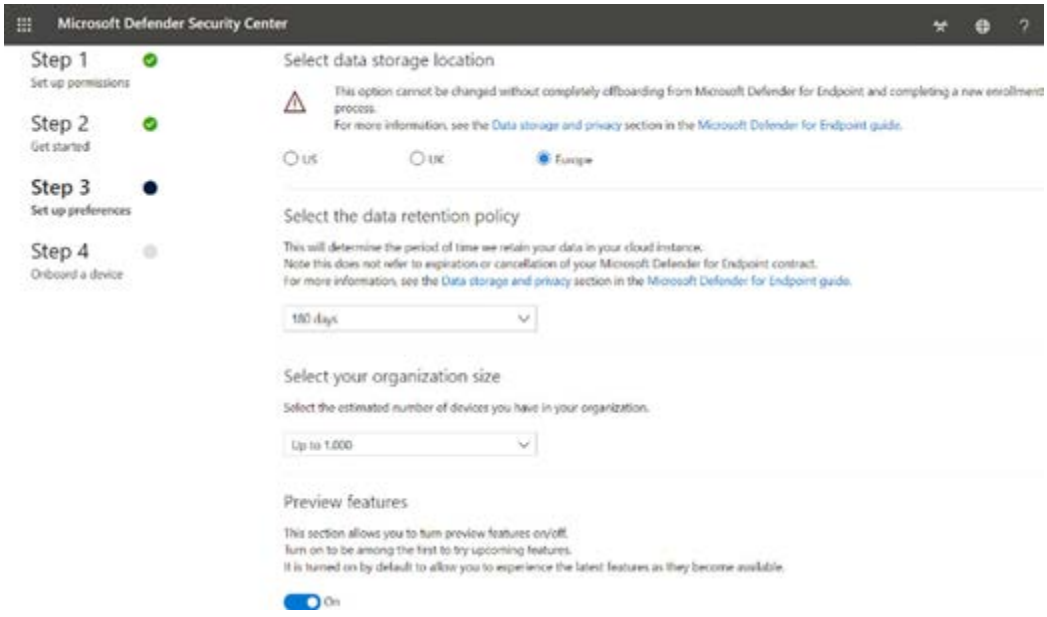


Figure 13.97: Microsoft Defender Security Center – Step 3

7. Make sure all the settings are correct, as there is no way back. Click on **Continue**.

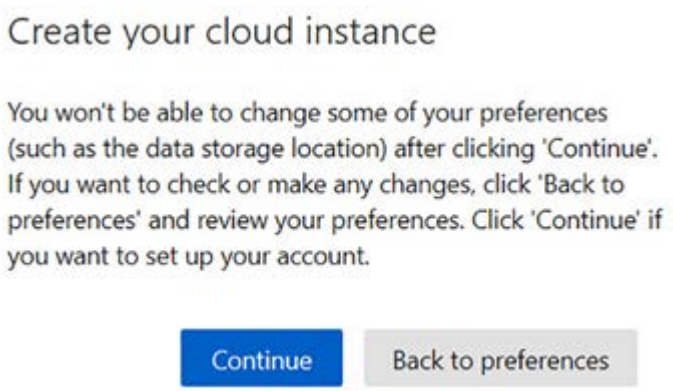


Figure 13.98: Create your cloud instance

8. Your Microsoft Defender for Endpoint account is being created. Please wait.

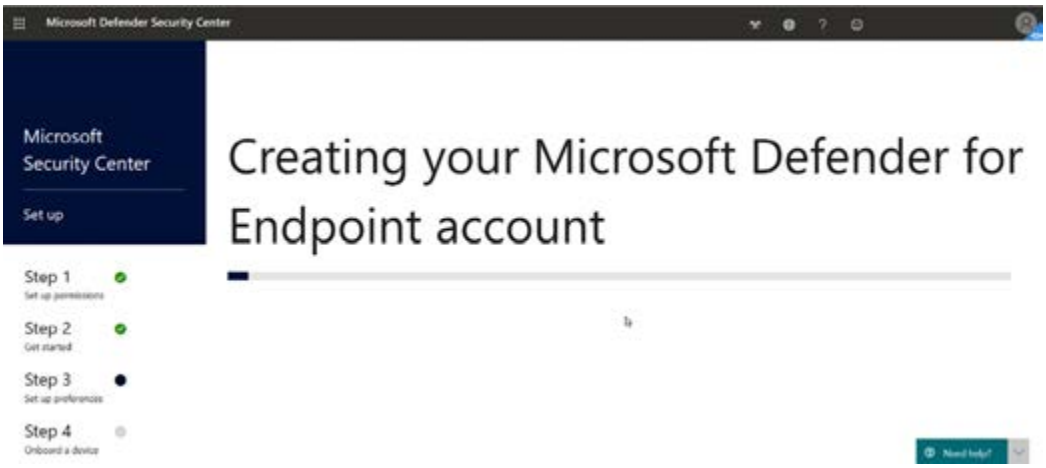


Figure 13.99: Microsoft Defender Security Center – Step 3

Now you are ready to create the Microsoft Defender for Endpoint integration with Microsoft Intune.

Connecting to Intune – Microsoft Intune integration

Follow these steps to proceed with the integration:

1. Open the Security Center portal: `https://securitycenter.windows.com/`.
2. Go to **Settings**.

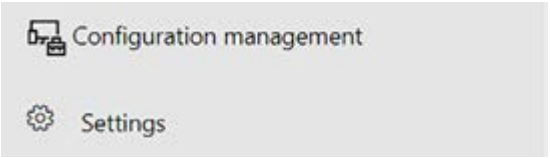


Figure 13.100: Settings

3. Turn the slider next to **Microsoft Intune connection** to **On**.

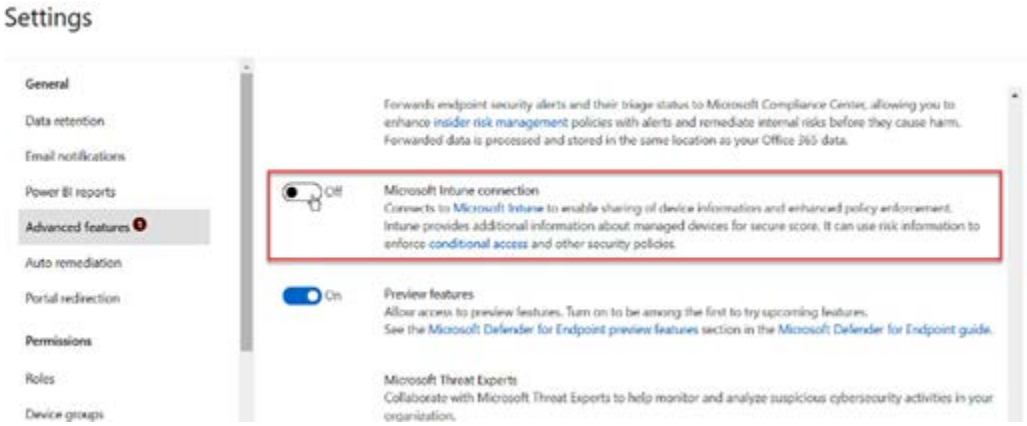


Figure 13.101: Microsoft Intune connection

4. Click on **Save preferences**.

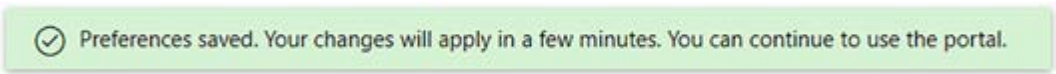


Figure 13.102: Preferences saved

5. At this point, Microsoft Defender integrates into Microsoft Intune. You can check the status in the **Endpoint security** menu.

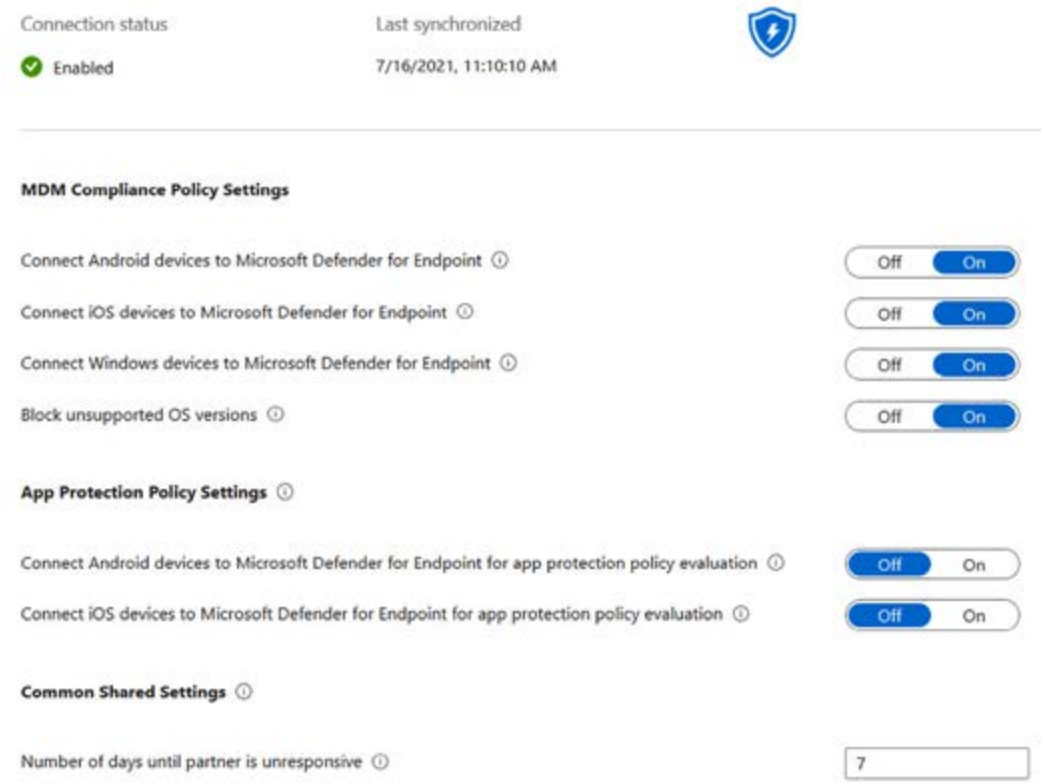


Figure 13.103: Connectors and tokens – Microsoft Defender for Endpoint

MDM Compliance Policy Settings: When on, compliance policies using the device threat level rule will evaluate devices, including data from this connector. When off, Intune will not use device risk details sent over this connector during device compliance calculation for policies with a device threat level configured. Existing devices that are not compliant due to risk levels obtained from this connector will also become compliant.

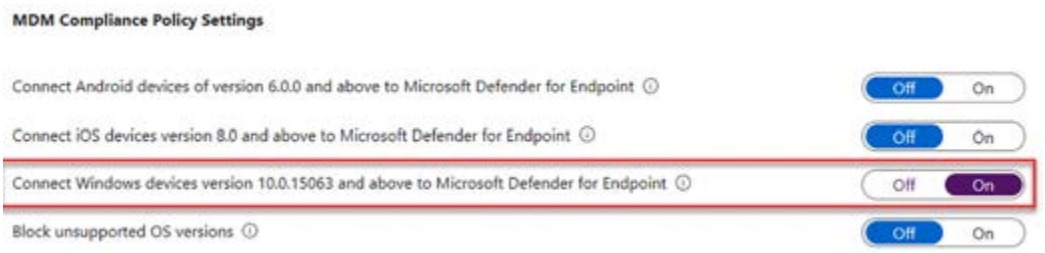


Figure 13.104: MDM Compliance Policy Settings

6. We now need to enroll our Windows endpoints into Defender.

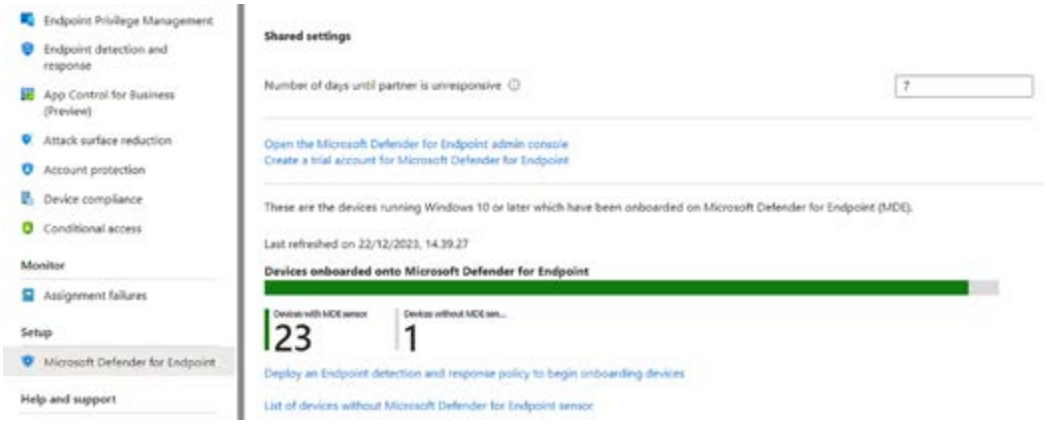


Figure 13.105: Windows devices – Microsoft Defender for Endpoint health state

7. Switch back to the Microsoft Intune portal.
8. Go to **Endpoint security**, followed by **Endpoint detection and response**.

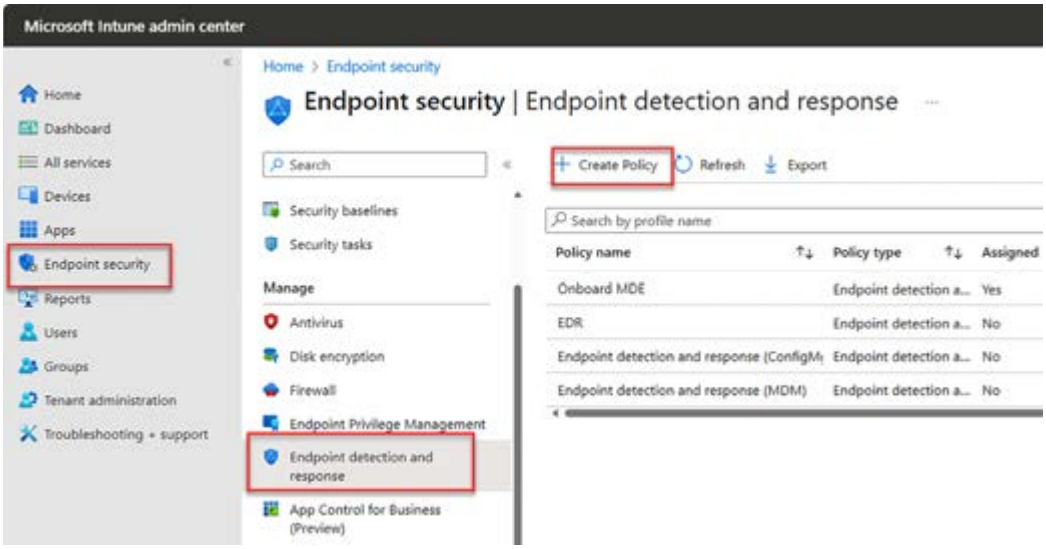


Figure 13.106: Endpoint detection and response

Before you start, download your Defender onboarding file:

1. You can find it in Defender, under **Settings | Onboarding**: `https://securitycenter.windows.com/preferences2/onboarding`.

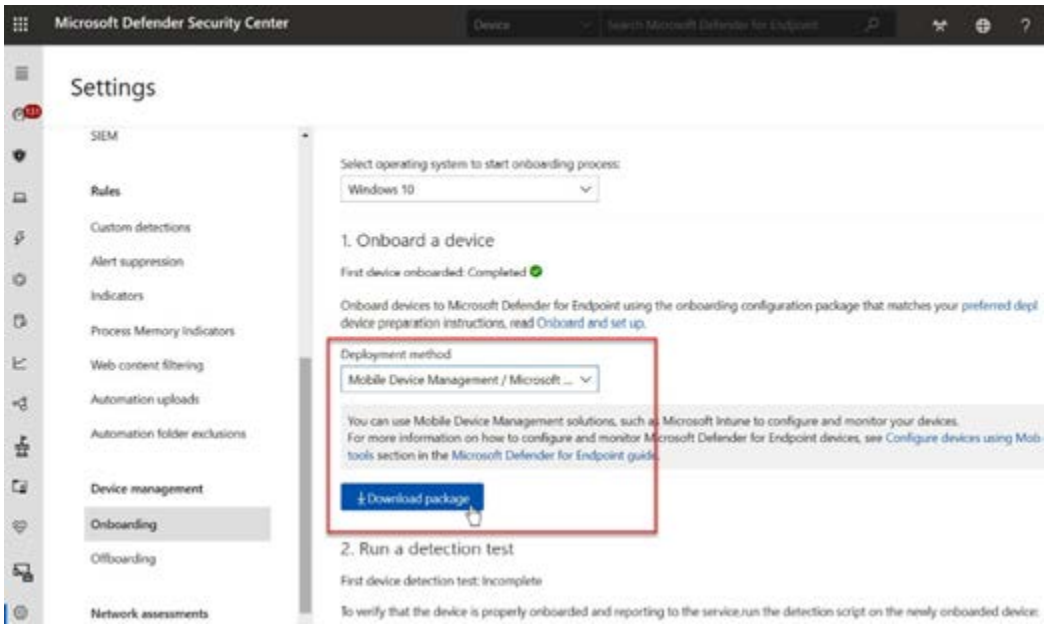


Figure 13.107: Downloading the onboarding file

2. Store it somewhere on your computer and unzip the folder.

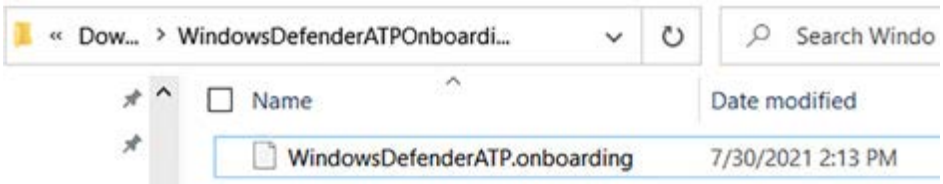


Figure 13.108: Saving the onboarding file

3. Select **Windows 10, Windows 11, and Windows Server and Endpoint detection and response** for the respective fields.

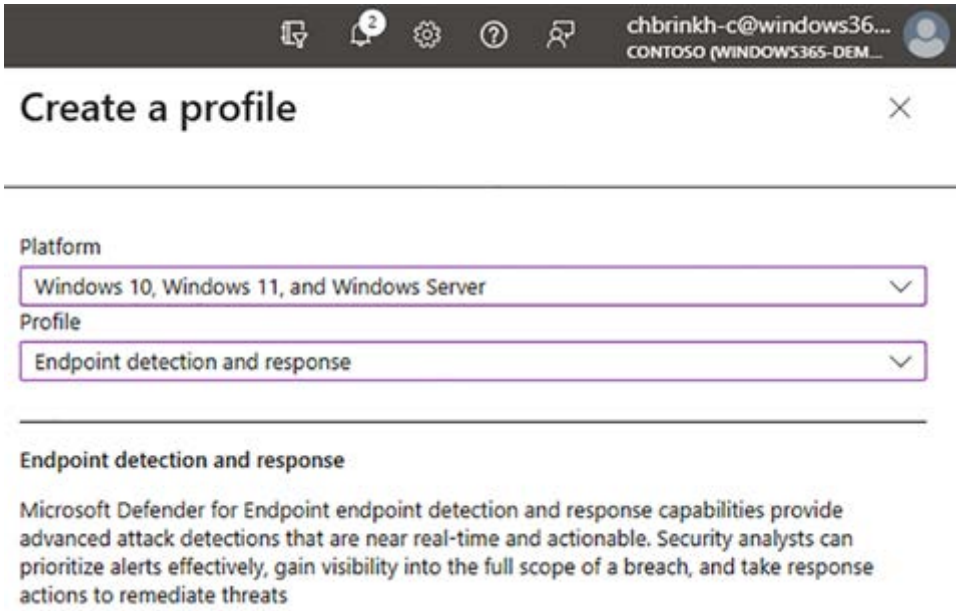


Figure 13.109: Endpoint detection and response (MDM) profile creation

4. Enter a name. Then, click **Next**.

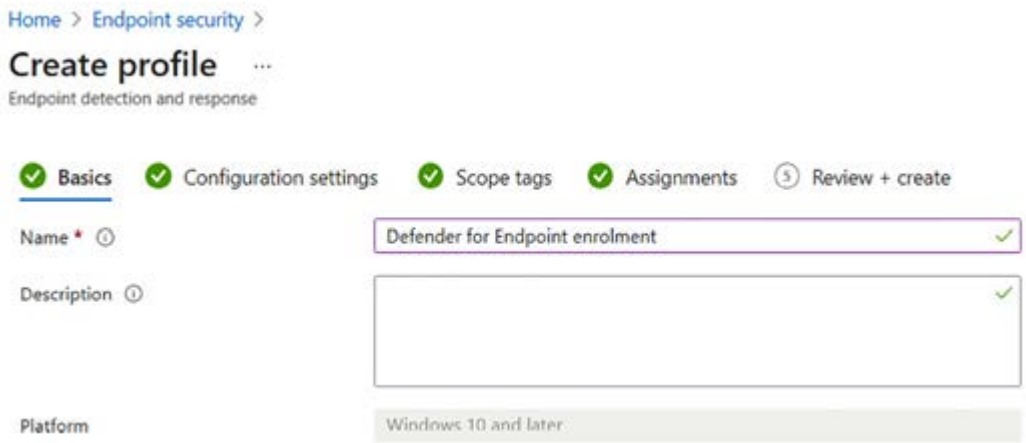


Figure 13.110: Create profile 1

5. If you have done the Intune integration, you can just leverage the option **Auto from connector**.

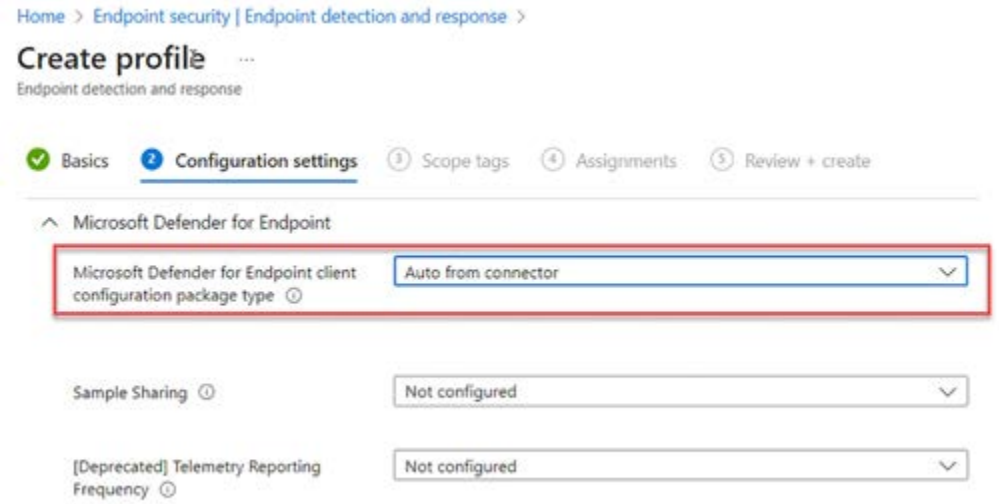


Figure 13.111: Auto from connector

If you have not configured the connector or you have Microsoft for Defender in another tenant, you can onboard with the following steps:

1. Enable the **Onboarding blob** setting.

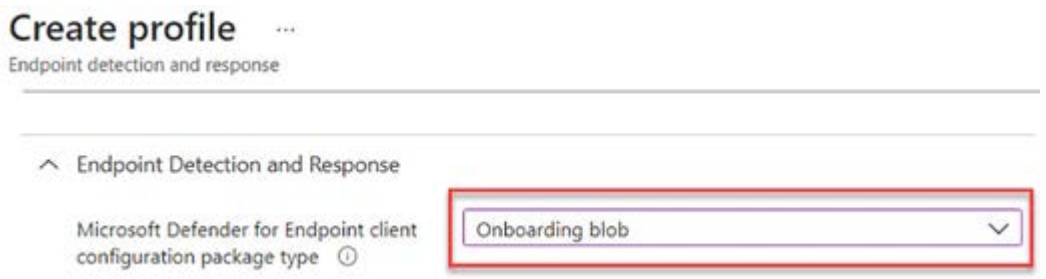


Figure 13.112: Create profile 2

2. Select the **WindowsDefenderATP.onboarding** file you downloaded earlier and upload it to your tenant.

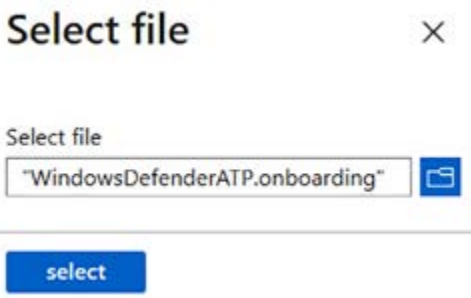


Figure 13.113: Uploading the onboarding file

3. Confirm that the onboarding file has been added correctly. This file includes the configuration that will be pushed to the endpoints so they know how to connect to your Defender for Endpoint tenant.

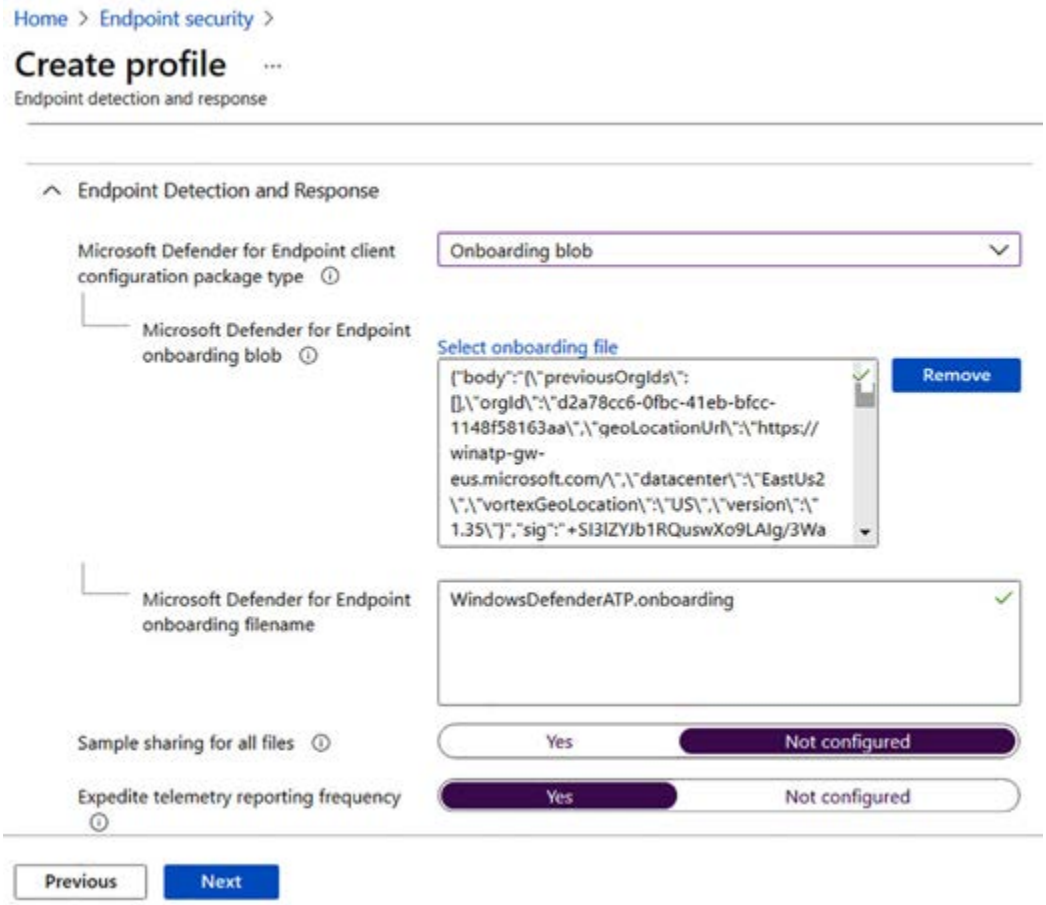


Figure 13.114: Creating an endpoint onboarding profile

4. Click **Next** (add scope tags if you are using them in your organization).

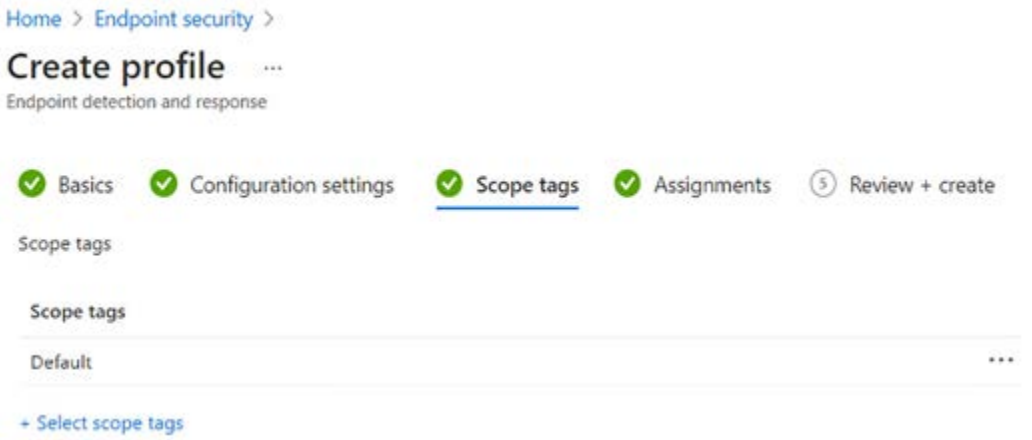


Figure 13.115: Scope tags

5. Click on **Add all users**. Then, click **Next**.

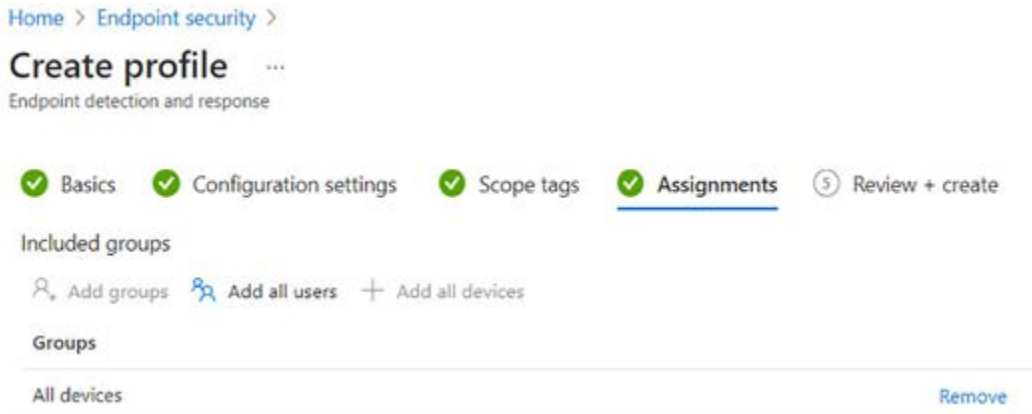


Figure 13.116: Assignments

6. Click on **Create**.

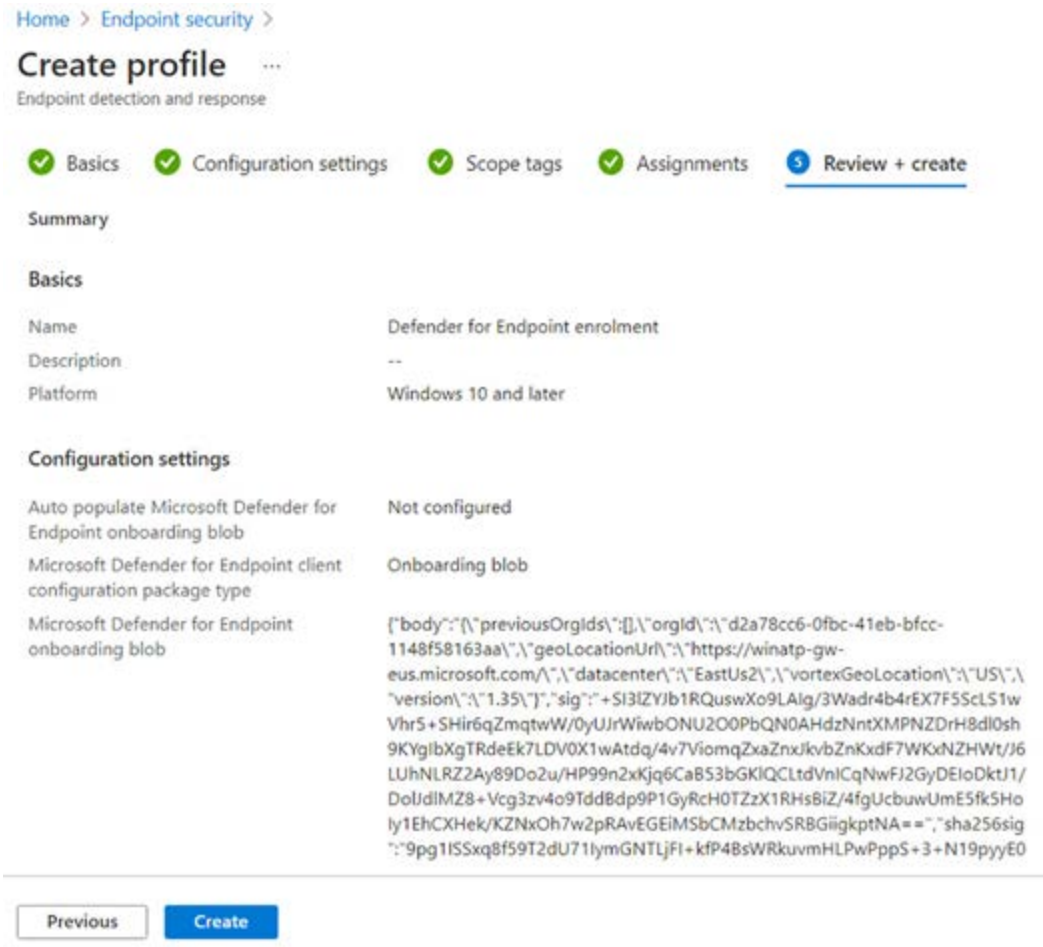


Figure 13.117: Creating the policy

7. Confirm that the rule is saying **Yes** under **Assigned.**



Figure 13.118: Endpoint detection and response

You should now see the status of your Windows virtual or physical endpoint changing from **Devices without Microsoft Defender for Endpoint Sensor** to **Devices with Microsoft Defender for Endpoint Sensor**.



The number of devices in this view only shows devices onboarded from the Microsoft Intune onboarding profile, not devices onboarded from scripts, Microsoft Endpoint Configuration Manager, or third-party tools.

Next, we will cover different options in Microsoft Defender Security Center.

Alerts and security assessments

Once the rollout and activation are done, and you have configured some security baselines and compliance profiles and assigned them to your desktops, you are ready to review your devices in the Microsoft Defender Security Center console. When you click on devices, you're able to drill down into the different assessments and alerts if any are detected.

Security recommendations

Microsoft Defender also recommends activating different features to increase the security level of your desktops in the **Security recommendations** tab. In there, you can find multiple settings that you can directly enable and push into Intune when you set up the connection correctly to your Intune tenant environment.

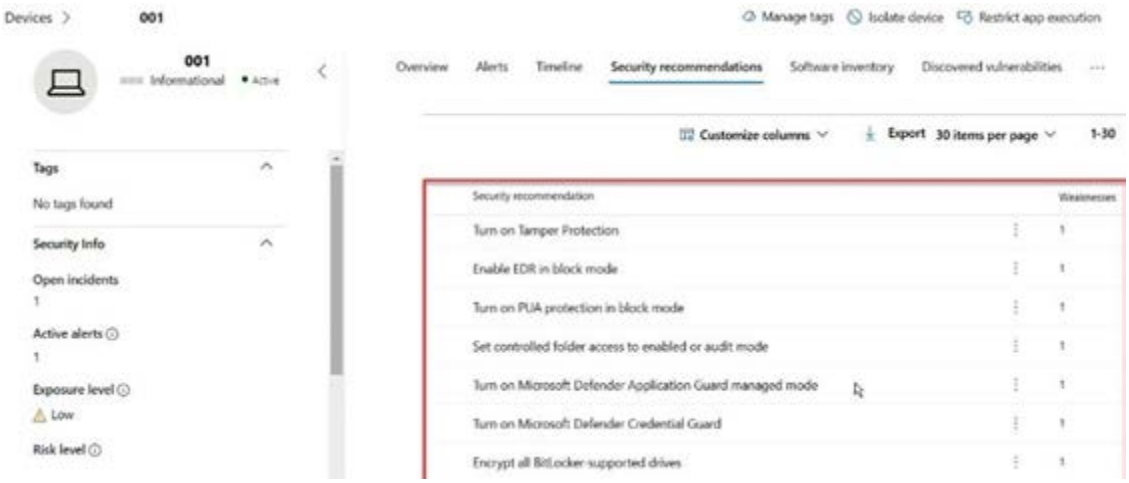


Figure 13.119: Security recommendations

Defender keylogger protection

Windows Defender for Endpoint now supports the detection of keyloggers, meaning, on managed endpoints connecting to Windows 365 Cloud PCs protected with Defender for Endpoint, software that tries to hijack the user's keyboard and mouse is no longer possible.

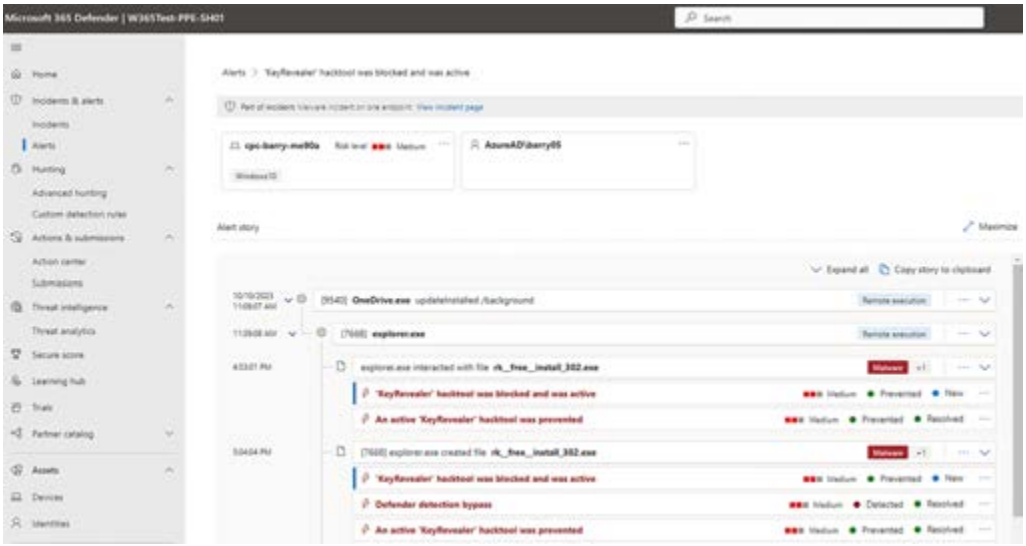


Figure 13.120: Keylogger protection

Windows 365: customer-managed keys support for data encryption

With Microsoft Purview Customer Key, customers can now use their own encryption key to protect their data at rest in cloud PC disks hosted in Microsoft's data centers.

This allows you as a customer to manage the customer keys while also ensuring that the OS disk of the Windows 365 Cloud PC is encrypted!

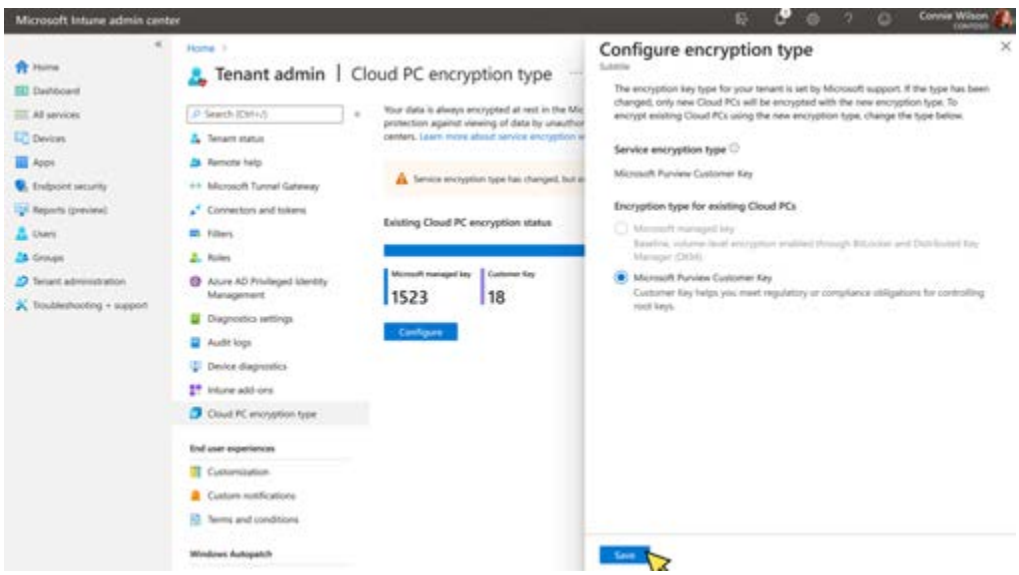


Figure 13.121: Cloud PC encryption type

Screen capture protection and watermarking

Screen capture protection, in conjunction with watermarking, serves as a safeguard against the capture of sensitive data on client endpoints via certain **operating system** (**OS**) features and **Application Programming Interfaces** (**APIs**). Activating screen capture protection automatically restricts remote content in screenshots and screen sharing.

Depending on your Windows version, there are two possible scenarios for screen capture protection:

1. **Preventing client screen capture**: The session host directs a compatible Remote Desktop client to activate screen capture protection for a remote session. This action blocks the client from capturing screen images of applications operating in the remote session.
2. **Preventing client and server screen capture**: The session host directs a compatible Remote Desktop client to activate screen capture protection for a remote session. This not only blocks the client from capturing screen images of applications operating in the remote session but also stops tools and services within the session host from capturing the screen.

When screen capture protection is active, users are unable to share their Remote Desktop window using local collaboration software like Microsoft Teams. This restriction applies to both the local Teams app and the use of Teams with media optimization for sharing protected content.

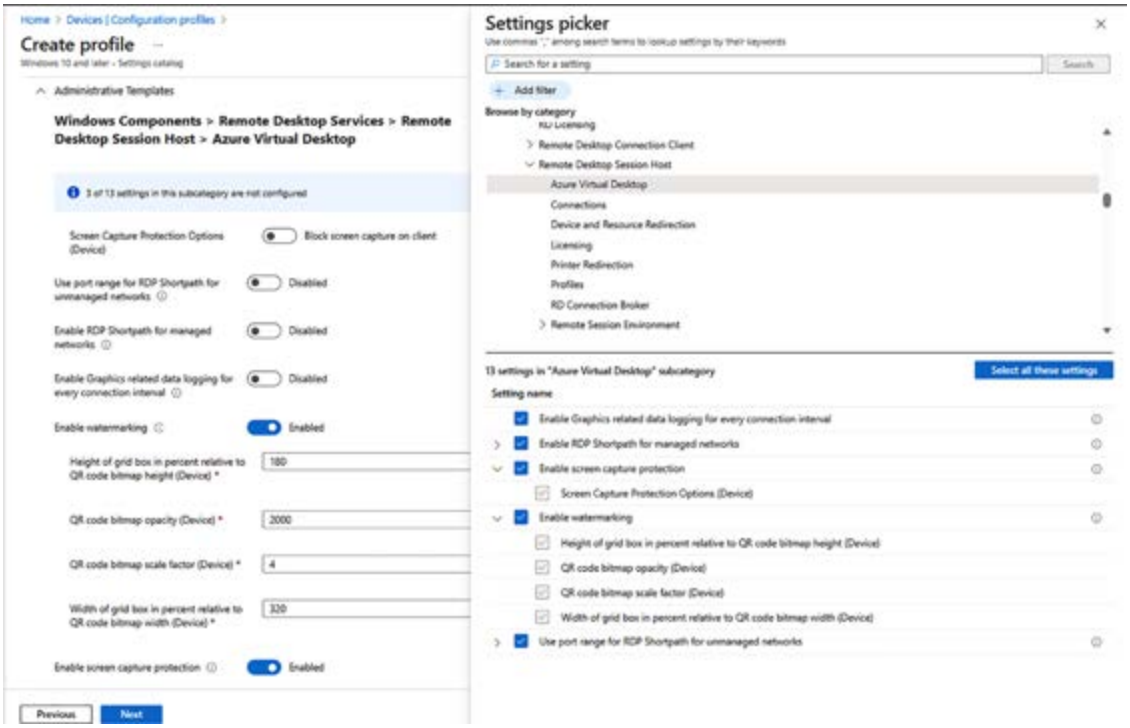


Figure 13.122: Screen capture protection and watermarking

Add a traceable watermark to cloud PCs – it will look like this for the end user after being enabled in Microsoft Intune.



Figure 13.123: Cloud PC watermarking

Summary

In this chapter, you've learned about the history of AD and about Entra ID, as well as what the options are to secure your identities better with Conditional Access and Microsoft Defender for Endpoint.

You learned how you can combine the force of Microsoft 365 E5 with device compliance on Microsoft Intune-managed devices with a Microsoft Defender for Endpoint risk score in a compliance policy to only allow access to corporate data by leveraging conditions all in the Microsoft Zero Trust security model.

In the next chapter, we're going to take a deeper dive into how to monitor your Windows Enterprise endpoints with endpoint analytics.

Questions

1. Do you need a license in order to use Azure MFA?
    a. Yes
    b. No
2. What configuration profile setting is required to configure your Windows devices for Microsoft Defender for Endpoint?
    a. Endpoint collections and response
    b. Security assessment
    c. Endpoint detection and response
    d. Sample sharing for all files

Answers

1. (b)
2. (c)

Further reading

If you want to learn more about Entra ID, Conditional Access, and Microsoft Defender for Endpoint after reading this chapter, please use one of the following free online resources:

- *Microsoft Defender for Endpoint – Microsoft Tech Community*: `https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/bg-p/MicrosoftDefenderATPBlog`
- *Practice security administration – Learn | Microsoft Docs*: `https://docs.microsoft.com/en-us/learn/modules/m365-security-threat-protect/practice-security-administration`

Get This Book's PDF Version and Exclusive Extras

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

***Note**: Keep your invoice handy. Purchases made directly from Packt don't require one.*

UNLOCK NOW

14

Monitoring and Endpoint Analytics

Monitoring your Windows environment is just as important as the implementation of it. User experience is the most important part of a successful implementation. After deploying your endpoints, it's important to ensure the performance and quality level of Windows and the applications that are part of your physical Windows and Windows 365 cloud PCs in your environment.

You will learn in this chapter how you can achieve this with Endpoint analytics, Productivity Score, and other monitoring capabilities of Microsoft Intune.

In this chapter, we'll go through the following topics:

- Endpoint analytics
- Advanced monitoring
- Top 10 processes impacting startup performance
- OS restart history
- Resource performance
- Insights and recommendations – score trends
- Application Reliability
- Windows 365-specific metrics
- Insights and recommendations
- Customizing your baselines
- Cloud PC performance dashboard
- System alerts and email notifications
- Cloud PC utilization
- Resize cloud PCs
- Productivity Score
- Service health
- Advanced Analytics
- ControlUp Enrich

Endpoint analytics

Endpoint analytics offers a way to gauge the performance of your organization's PCs and the quality of user experience being delivered by you, the IT administrator. It can assist in pinpointing policy or hardware problems that might be causing device slowdowns, high-latency connections, or other issues.

This allows you to proactively implement solutions before users need to submit a help desk ticket. Endpoint analytics can be found in the Microsoft Intune admin center portal, in the **Reports** section.

If you are an existing Microsoft Intune customer, you'll already use the **Monitor** option inside the **Devices** menu. As Windows 365 is equal to a physical Windows 10 Enterprise desktop, you can monitor both your virtual and physical devices here for one unified experience.

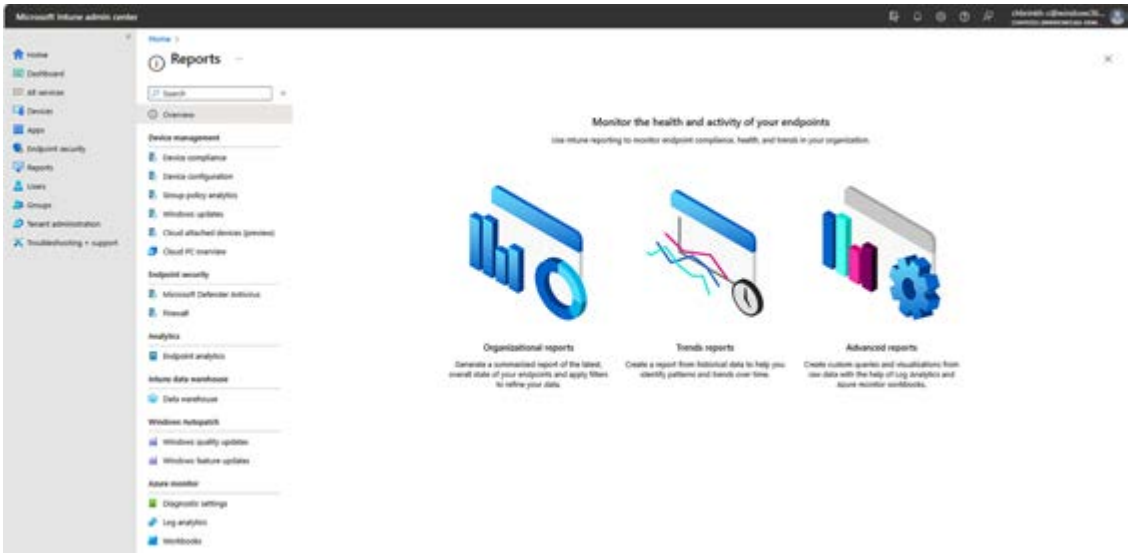


Figure 14.1: Intune admin center – Endpoint analytics dashboard

You can gather insights about your environment as well as think about metrics such as **app licenses**, **discovered apps**, **app install**, and **app protection statuses**.

Here's a full rundown of the different monitoring dashboards available:

- **Configuration**:
    - Assignment status
    - Assignment failures
    - Devices with restricted apps
    - Encryption report
    - Certificates
- **Compliance**:
    - Non-compliant devices

    - Devices without compliance policy
    - Setting compliance
    - Policy compliance
    - Non-compliant policies
    - Windows Health Attestation report
    - Threat agent status
- **Enrollment:**
    - Autopilot deployments
    - Enrollment failures
    - Incomplete user enrollments
- **Software updates:**
    - Per-update ring deployment state
    - Installation failures for iOS devices
    - Feature update failures
    - Windows expedited update failures
- **Other:**
    - Device actions

You could, for example, easily find out what apps are being deployed and how many are successful, as in the example in the following section.

Cloud PC overview

In the Reports dashboard menu, you can now easily find the issues that potentially are happening in your Windows 365 environment. This new dashboard will show you a summary of the **Connection quality**, **Cloud PC utilization**, **Connected Frontline Cloud PCs**, and **Cloud PC recommendations** (more about this later).

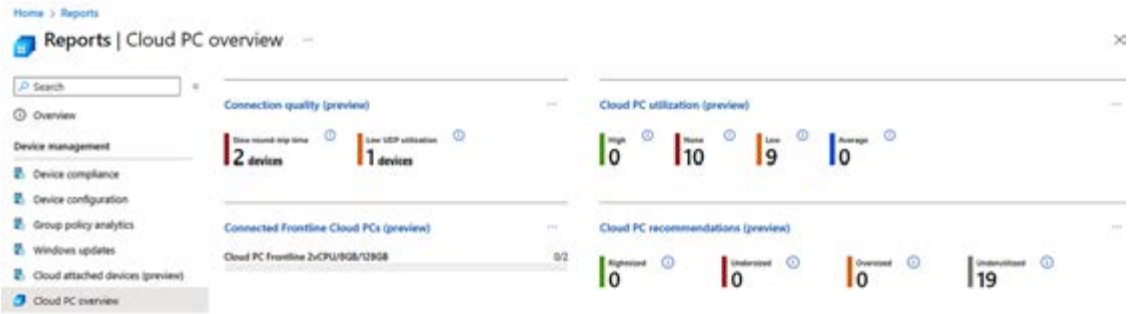


Figure 14.2: Cloud PC overview

Cloud attached devices (preview)

This new dashboard will show all your cloud attached devices per Configuration Manager, attached to Microsoft Intune.

Other attributes such as compliance status, device configuration, endpoint protection, Windows Updates, and many more are in here too.

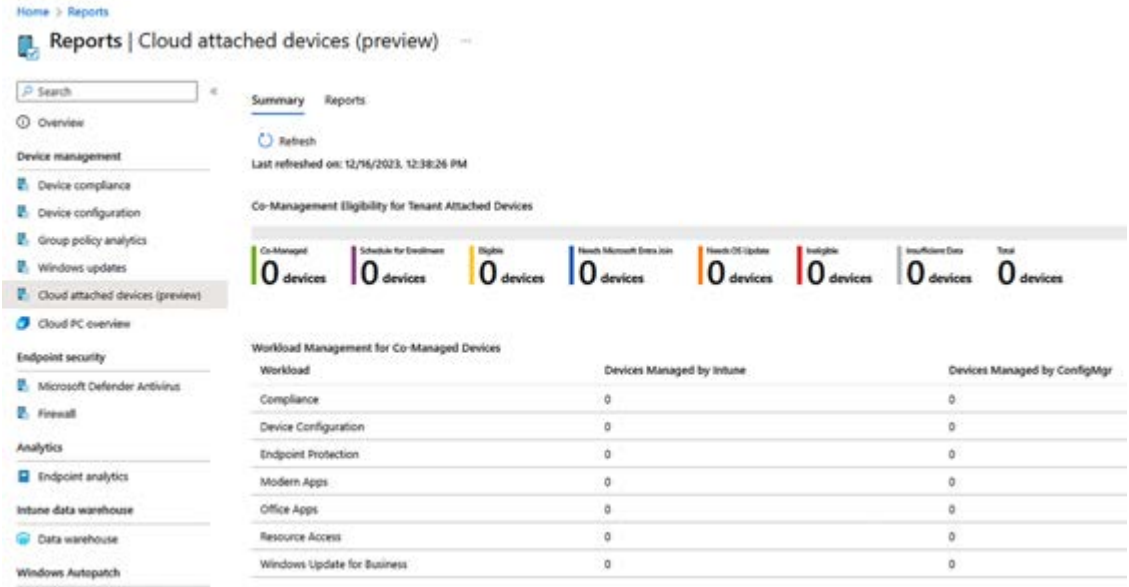


Figure 14.3: Cloud-attached devices (preview)

Endpoint analytics – Advanced Monitoring

The main purpose of Endpoint analytics is to proactively optimize the user experience and track your progress along the way. It's your main dashboard as an IT administrator to track the quality level of both your physical and virtual desktop environments.

The metrics that you can find show the value of all Microsoft Intune-managed devices in your environment, for example, the values of your physical and Windows 10 or 11 cloud PCs combined.

Here's a list of the reports/dashboards currently available in Endpoint analytics:

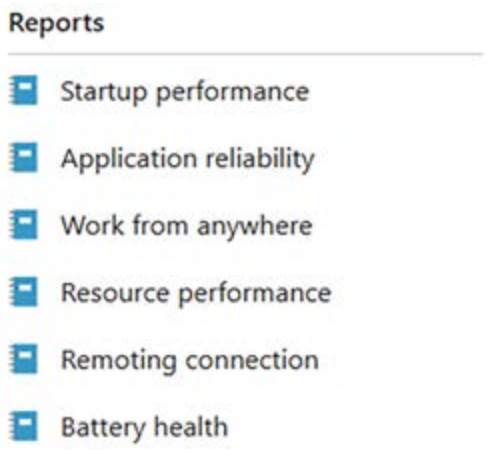


Figure 14.4: Reports

You can find the overall status of your environment within Endpoint analytics under Reports | Endpoint analytics in Microsoft Intune.

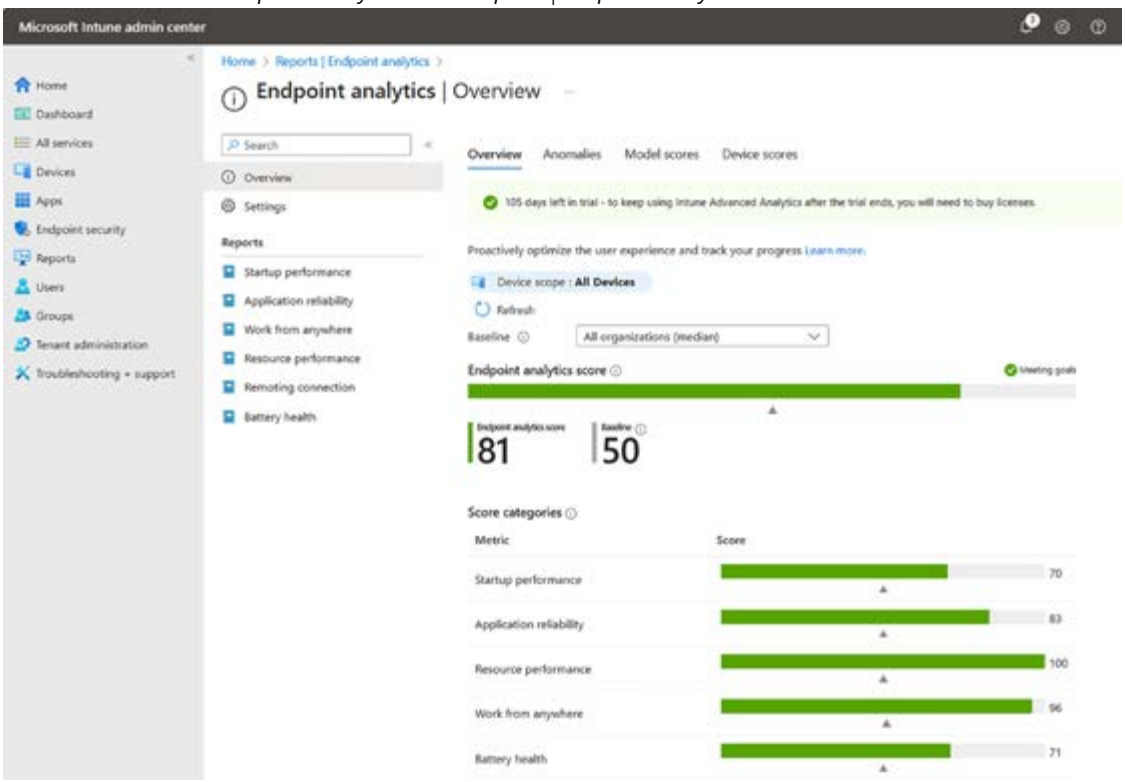


Figure 14.5: Overview of your environment

Startup performance – logon duration

Improving startup performance to optimize the time from powering on your physical computer to productivity is best for consistent performance in terms of increasing the speed to productivity.

Review your current score and see how it compares to the selected baseline. Refer to the list of different insights and recommendations to learn how to improve your device startup times and score; this can be found in the Endpoint analytics dashboards.

Here's a list of the metrics available in Endpoint analytics, per organization, and per user device level, to dig deeper into specific scenarios:

- **Core boot**: Average time it takes to reach the sign-in prompt after a device is turned on. Excludes the OS update time:
    - **Group Policy**: Average time spent processing Group Policy during the device's core boot
    - **To sign-in screen**: Core boot time minus the time spent processing Group Policy
- **Core sign-in**: Average time it takes to get to a responsive desktop after a user signs in. Excludes new user sign-in and first sign-in following a feature update:
    - **Group Policy**: Average time spent processing Group Policy during the device's core sign-in
    - **To desktop**: Average time between sign-in and when the desktop renders, minus the time spent processing Group Policy
    - **To responsive desktop**: Average time between when the desktop renders and when CPU usage falls below 50%

The startup performance score gives the IT department insight into the end-user experience from power-on to productivity. With these insights come recommendations on what to change to improve end users' experience. Next, we will cover the performance score breakdown.

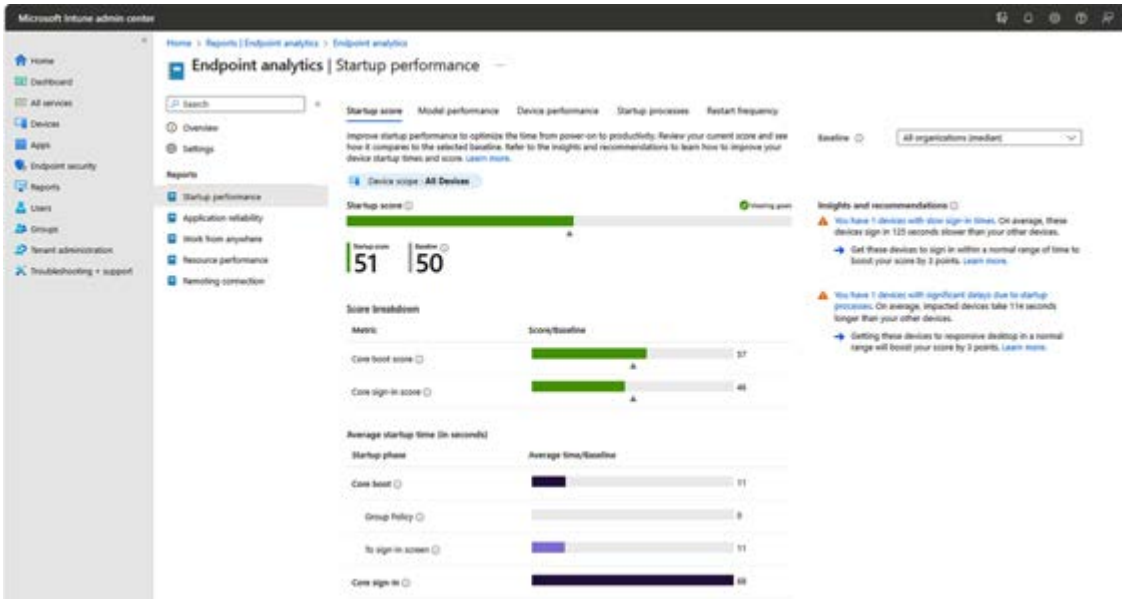


Figure 14.6: Startup performance

Performance score breakdown

To calculate our tenant's score, we look at how long it takes each device to complete the core boot phase and score each experience from 0 (poor) to 100 (exceptional). We then calculate the average score of all devices to get the core boot score.

In the following screenshot, you can find an example breakdown of the full logon process, from booting up, to even further in your cloud PC, your Windows 10 Enterprise endpoint.

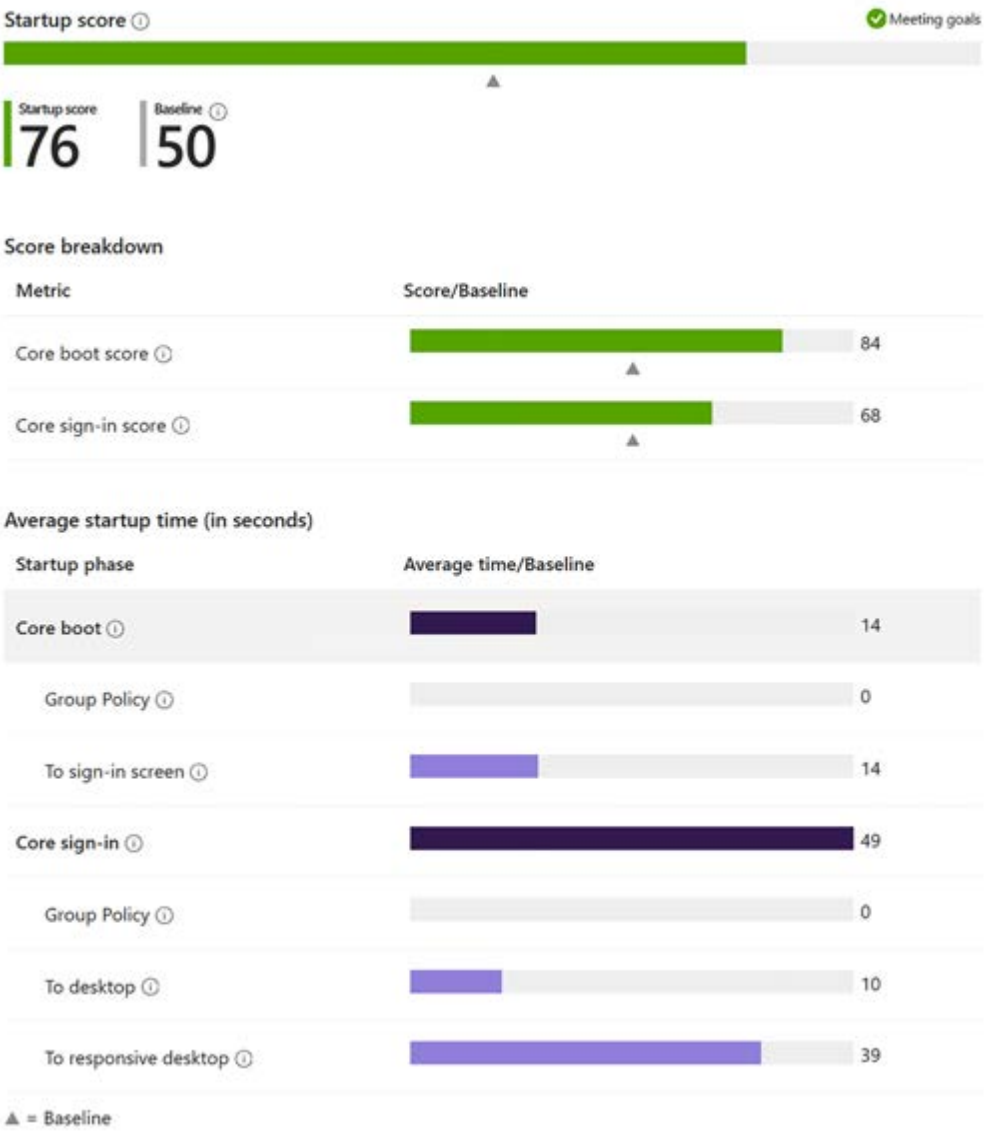


Figure 14.7: Performance score

If you need to see the individual status of a single Windows 10 physical or cloud PC, you can go to **Endpoint analytics | Reports | Startup performance | Device performance.**

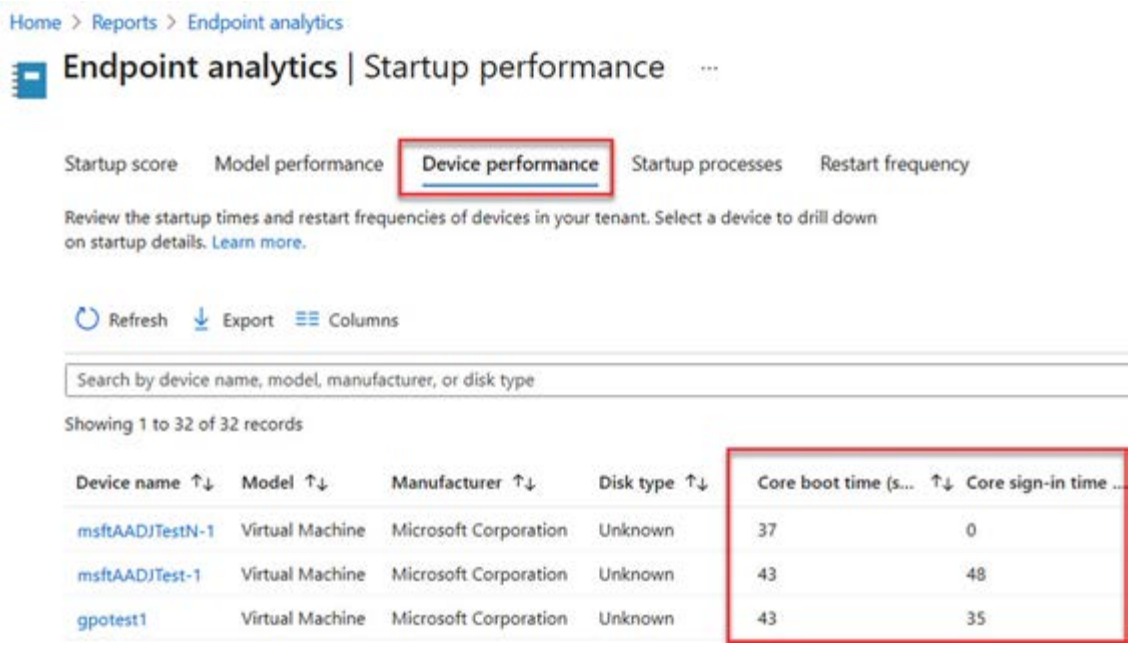


Figure 14.8: Device performance

Once you click on the device name, different individual metrics are shown. Here, you can find the logon duration and boot history of your endpoints.



NOTE

The sign-in history is segmented to make it easier to find the potential root cause of the delay.

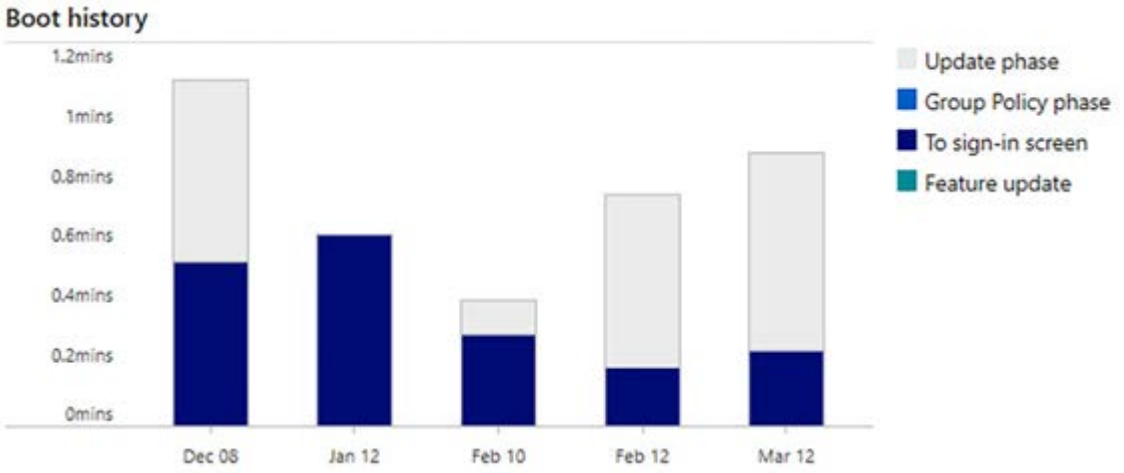


Figure 14.9: Boot history

You can also find the sign-in history here if you scroll a little further down. This is the easiest method to track whether performance has decreased (or not).

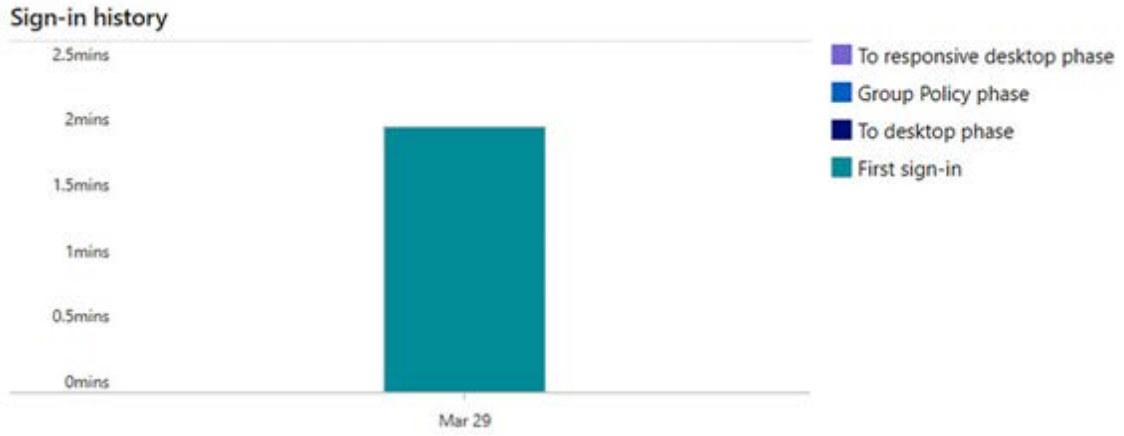


Figure 14.10: Sign-in history

Resize cloud PCs

The requirements for applications and functions from users may evolve, potentially necessitating more hardware power for them to accomplish their tasks and maintain a positive user experience on their cloud PC. Conversely, users might have a high-spec cloud PC that doesn't require as much power.

Windows 365 includes a feature that allows you, as an IT administrator, to resize cloud PCs. Before resizing a cloud PC, ensure you have the appropriate Windows 365 license **Stock-Keeping Unit** (**SKU**), also known as a license, you wish to assign to the user. Initiating a resize will remove all restore points.

Bear in mind that resizing a cloud PC will cause it to restart and disconnect the user. It's important to coordinate with the user before resizing to avoid losing any unsaved work.

If your cloud PC is performing badly and is causing a lot of CPU spikes, Endpoint analytics will suggest you resize your cloud PC. This is a new, proactive method to ensure the performance of your end users.

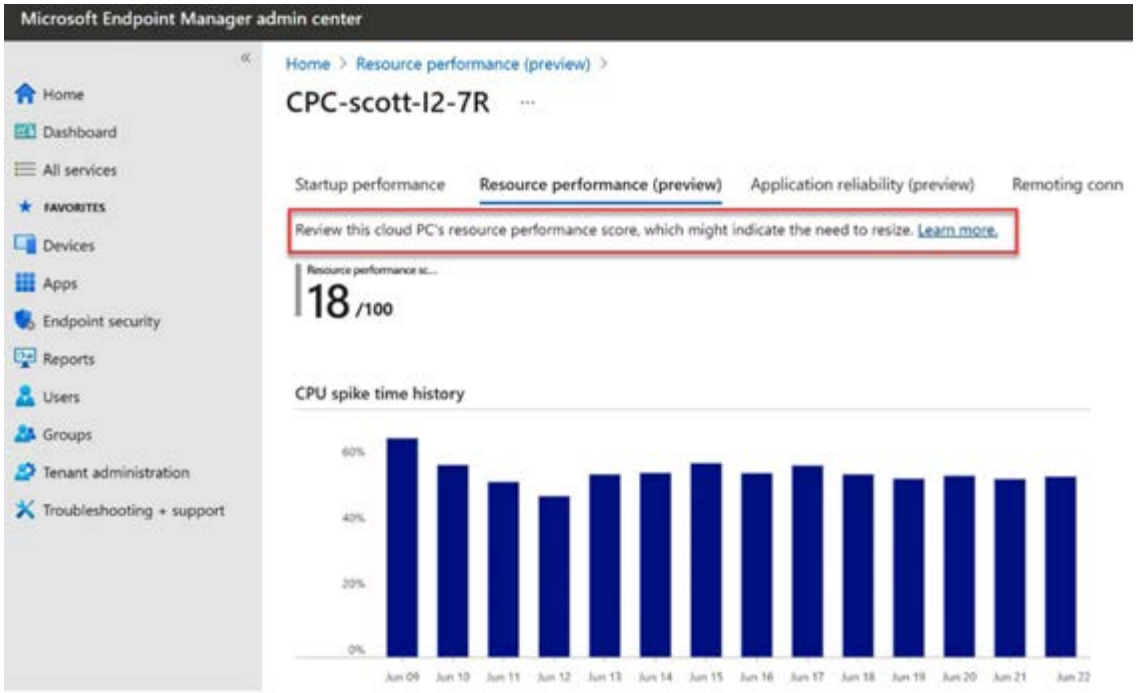


Figure 14.11: Resource performance

You can find this feature (in preview) in the Microsoft Intune portal, under **Devices**; select the **Resize** button, as seen in the following screenshot:

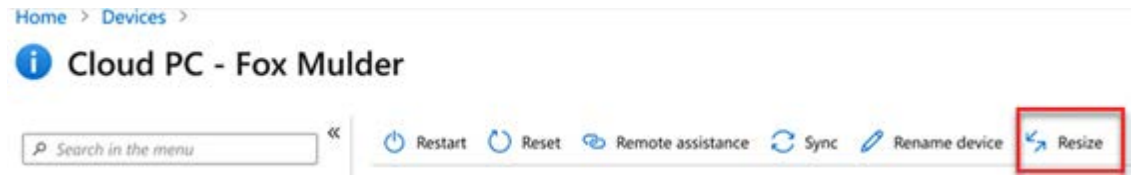


Figure 14.12: Resize feature

When you click **Resize**, you will be taken to the following screen:

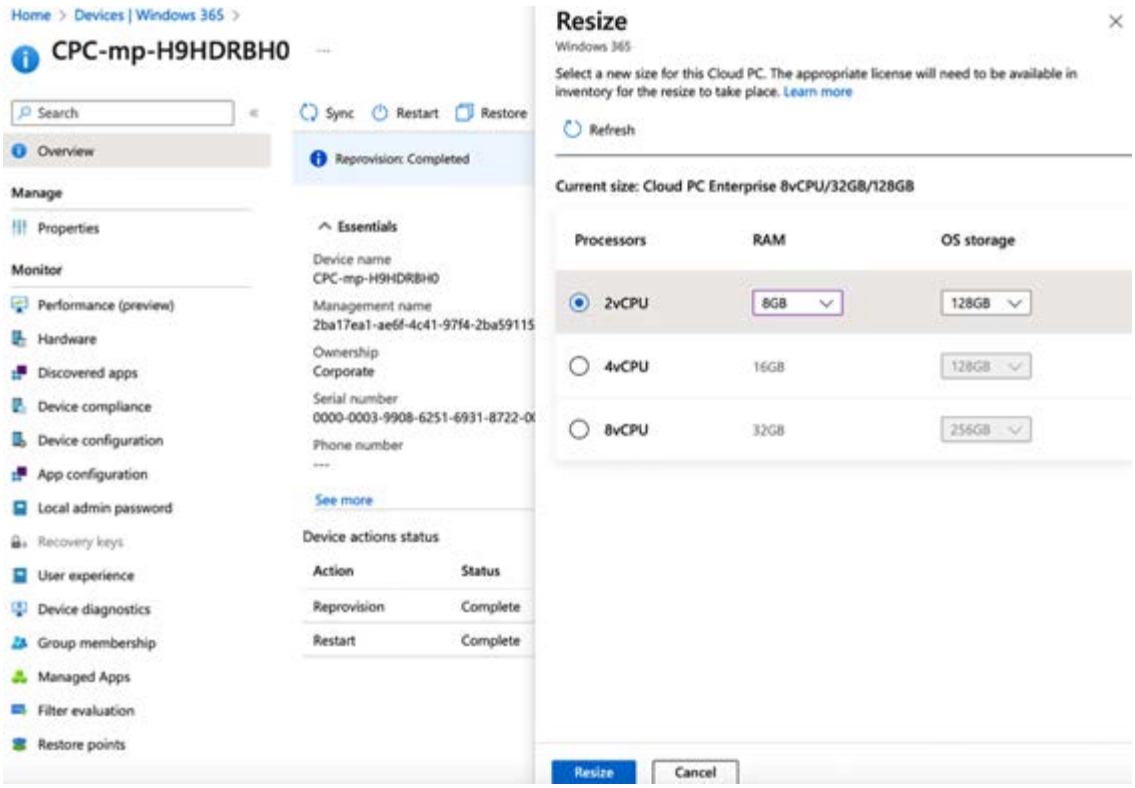


Figure 14.13: Resize

In this section, we covered Endpoint analytics reporting for Windows 365, as well as how you can resize your cloud PCs to provide them with more CPU and RAM resources. Next, we will look more closely into some of the detailed data you can get on your Windows devices with Endpoint analytics.

Top 10 processes impacting Startup performance

In **Startup performance** on the **Device performance** blade, you can select a single device where you can show the top 10 processes that have the most impact on the device's startup performance.

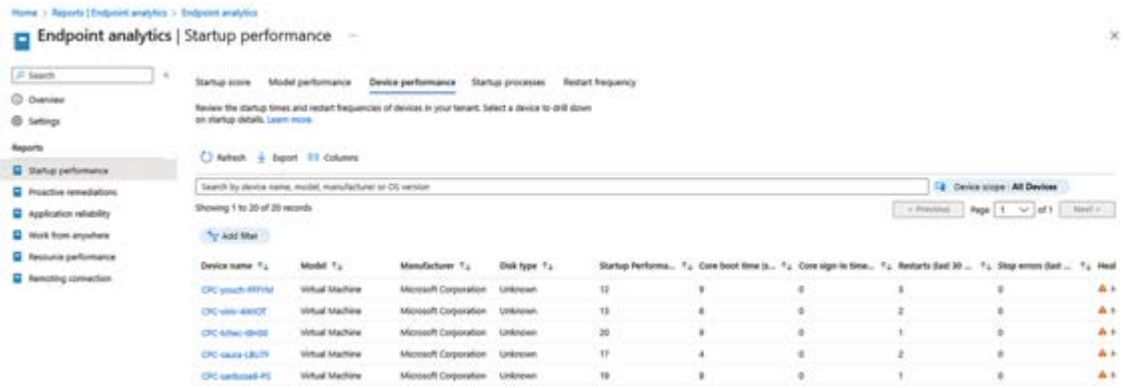


Figure 14.14: Startup performance

This data is also visible in the **Device** blade if you go into a specific device and then to **Monitor | User Experience.**

Top 10 impacting startup processes

Process name	Description	Publisher	Impact (seconds)
WmiPrvSE	WMI Provider Host	Microsoft Corporation	6
omadmclient	Windows MDM Client	Unknown	5
svchost-netsvcs	Service Host: netsvcs	Microsoft Corporation	1
svchost-RPCSS	Service Host: RPCSS	Microsoft Corporation	1
svchost-UnistackSvcGroup	Service Host: UnistackSvcGroup	Microsoft Corporation	1
svchost-DcomLaunch	Service Host: DcomLaunch	Microsoft Corporation	1
svchost-LocalSystemNetworkRestricted	Service Host: LocalSystemNetworkRestri...	Microsoft Corporation	1
svchost-LocalServiceNetworkRestricted	Service Host: LocalServiceNetworkRestri...	Microsoft Corporation	1
svchost-AppReadiness	Service Host: AppReadiness	Microsoft Corporation	1
svchost-LocalServiceNoNetwork	Service Host: LocalServiceNoNetwork	Microsoft Corporation	1

Figure 14.15: Top 10 impacting startup processes

OS restart history

Last but not least, you can also find the restart actions on each physical and cloud PC in the last section of the dashboard:

OS restart history

Date	OS version	Restart category	Stop code	Failure bucket Id
03/30/21	10.0.19042.867	Update		
04/15/21	10.0.19042.928	Update		

Figure 14.16: OS restart history

Resource performance

In this dashboard, it's possible to see the application events on your physical and cloud PCs. This gives you insights into one of the most important indicators of bad user experience – CPU and RAM utilization.

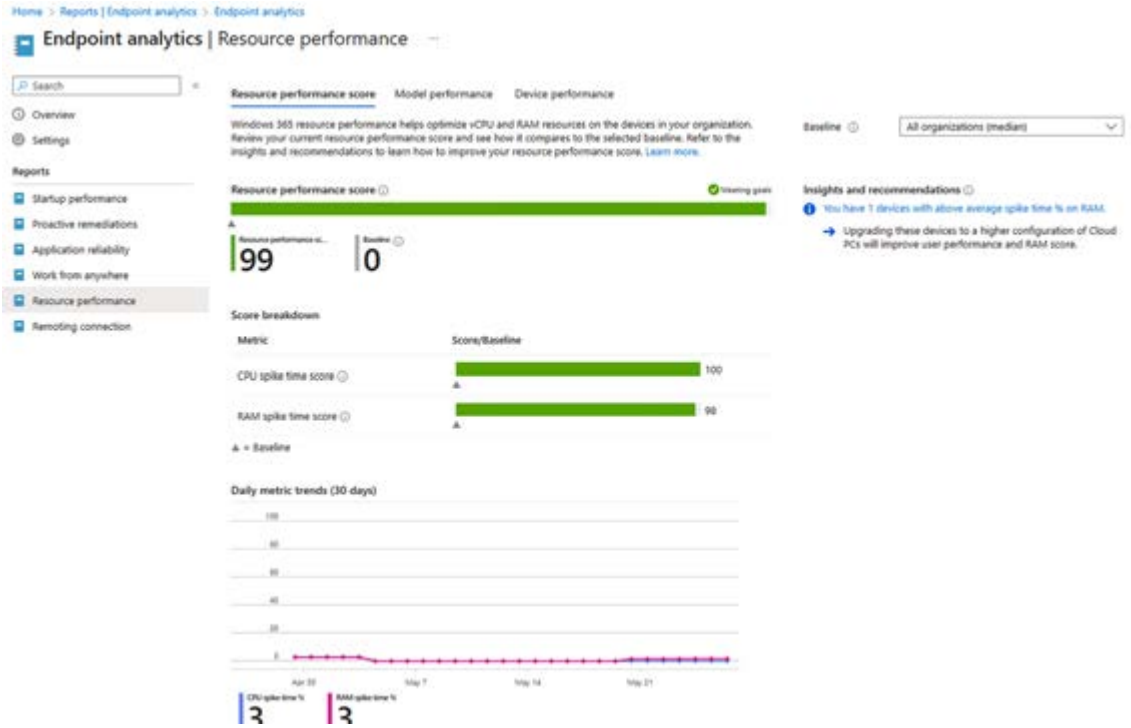


Figure 14.17: Resource utilization

Insights and recommendations – score trends

It's also possible to see the last 30 days of resource consumption and whether there's a trend. This would make it easy, when you provide a fix, to see whether the improvement affects all your users.

Also, the other way around, when issues occur or you install an update that requires way more resources than before, you can start correlating your results with the time of enrollment of that patch or update. Very insightful.

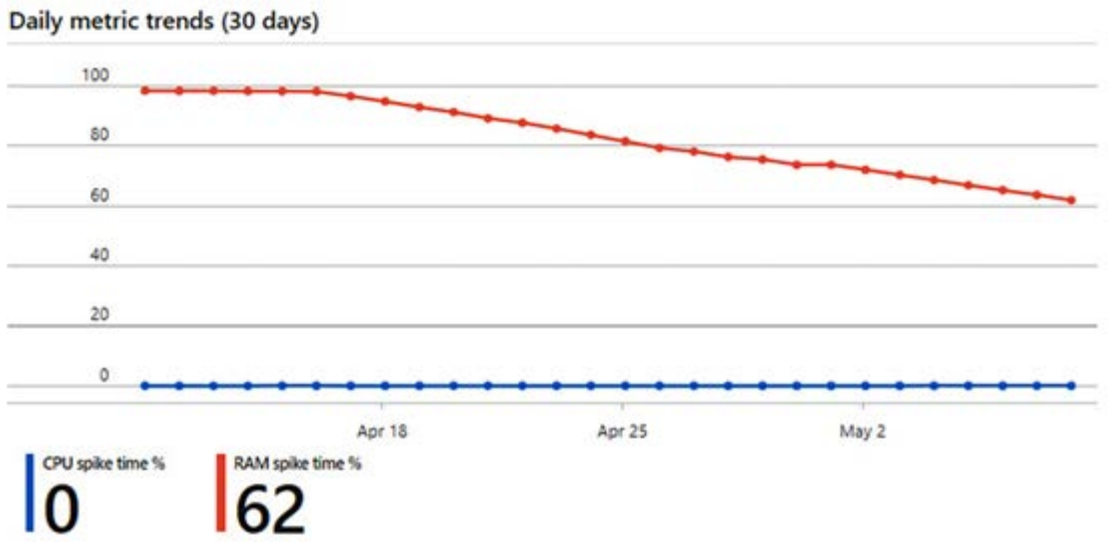


Figure 14.18: Score trends

Application reliability

Healthy, performant applications enable users in your organization to be productive. Review your current app reliability score and see how it compares to the selected baseline.

Refer to the insights and recommendations to learn how to improve your app reliability score.

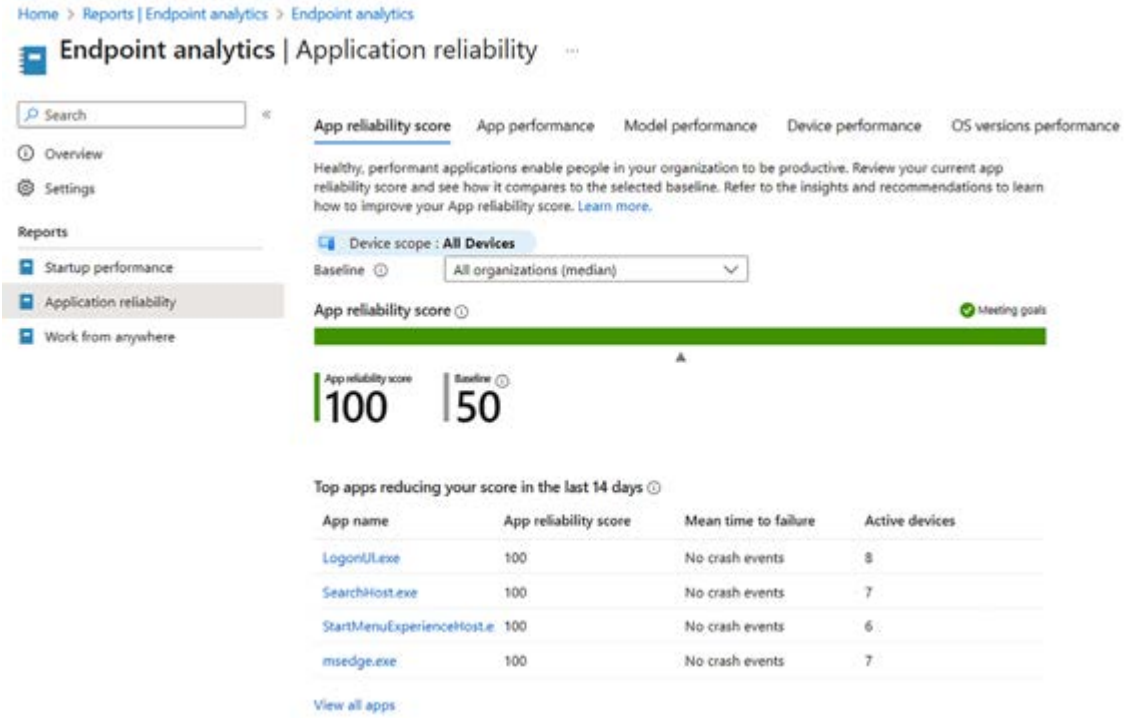


Figure 14.19: App reliability score

App reliability score provides IT admins with a high-level view of desktop application robustness across your environment. App reliability score is a number between 0 and 100. The score is calculated from the app reliability scores of each desktop application in your environment that's found in the **App performance** tab.

Each application on the **App performance** tab is assigned an app reliability score based on the following:

- **Crash frequency**: For each app, there are two metrics:
    - The total number of app crashes.
    - The total usage duration over a 14-day rolling window is used to calculate the Mean time to failure value in the **App performance** tab.
- **Total usage duration**: This is a factor in the usage duration across all enrolled devices in Endpoint analytics. This ensures that you get the data for the most disruptive application issues that are prioritized in the App reliability score.

Windows 365-specific metrics

Another huge benefit is that Endpoint analytics is also the tool you use to check the status of your physical endpoints. This means that you can create one single pane of glass to check the status of your physical endpoint and cloud PC endpoint altogether at once.

There are six new Windows 365 Endpoint analytics categories to measure the performance of your environment:

- **Resource performance:**
  - CPU spike time percentage
  - RAM spike time percentage
- **Remoting connection:**
  - RD client login time
  - RD client login failure
  - **Round Trip Time (RTT)**

The following screenshot is an example of measuring the latency of the connection to your Windows 365 cloud PC environment:

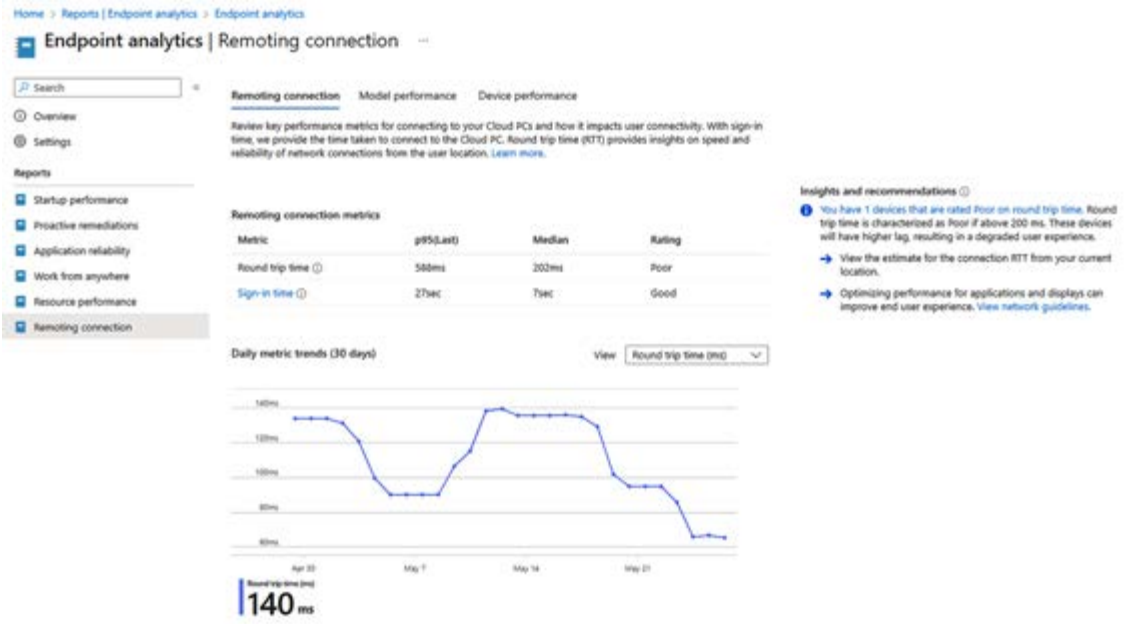


Figure 14.20: Remoting connection metrics

The following are the kinds of metrics that are available to measure startup performance and logon duration:

- **Startup performance:**
  - Boot time for Windows 365 cloud PC endpoint
  - Login time for Windows 365 cloud PC endpoint

The following are insights into the boot time, logon duration, and round-trip time (RTT – latency) of both your physical and cloud PC environment.



Figure 14.21: Startup performance

- **Proactive remediations:**
  - Automated actions to remediate common issues with a Windows 365 cloud PC
- **Recommended software:**
  - Windows version
  - Cloud identity
  - Cloud management
  - Cloud provisioning
- **Application health:**
  - Cloud PC app usage and crashes

Insights and recommendations

Endpoint analytics also gives you advice when it detects performance issues in your environment. For example, if, on the resource performance dashboard, over 90% CPU usage is detected, it recommends upgrading your cloud PC. This could also apply to physical PCs.

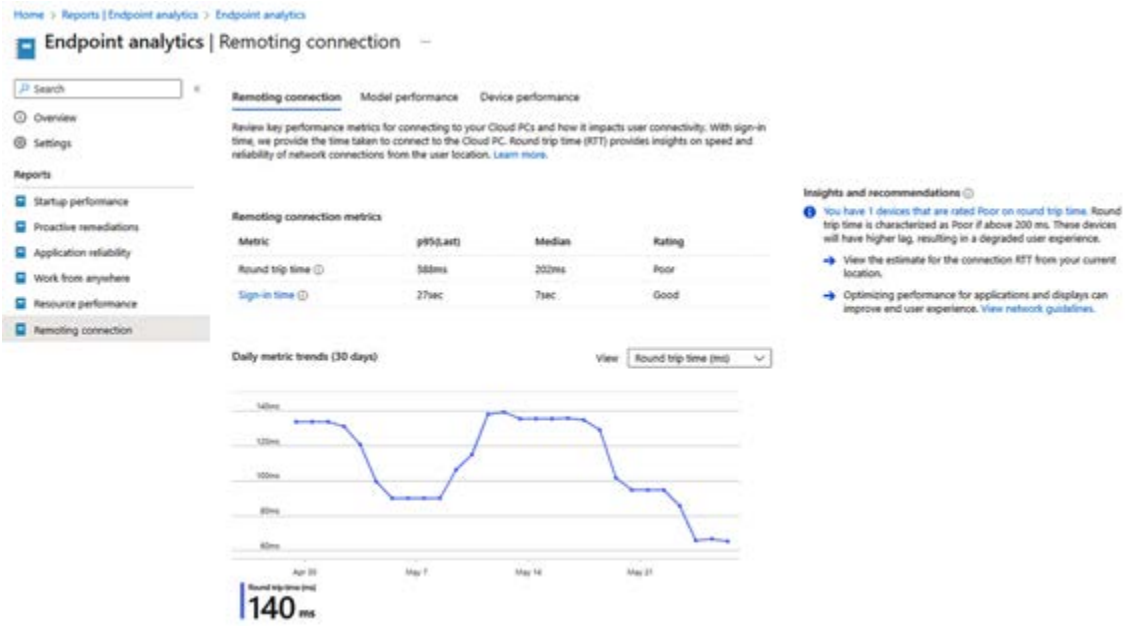


Figure 14.22: Recommendation

Configuration Manager data collection

You could also collect user experience data from devices managed by Microsoft Endpoint Configuration Manager to calculate scores and insights. We explain the steps to enable tenant attachment and co-management in *Chapter 6*, *Windows Deployment and Management*.

In the **Endpoint analytics | Settings** menu, you can find out whether the connection works properly. If not, as in the following example, no data will be shown in Endpoint analytics coming from Configuration Manager.

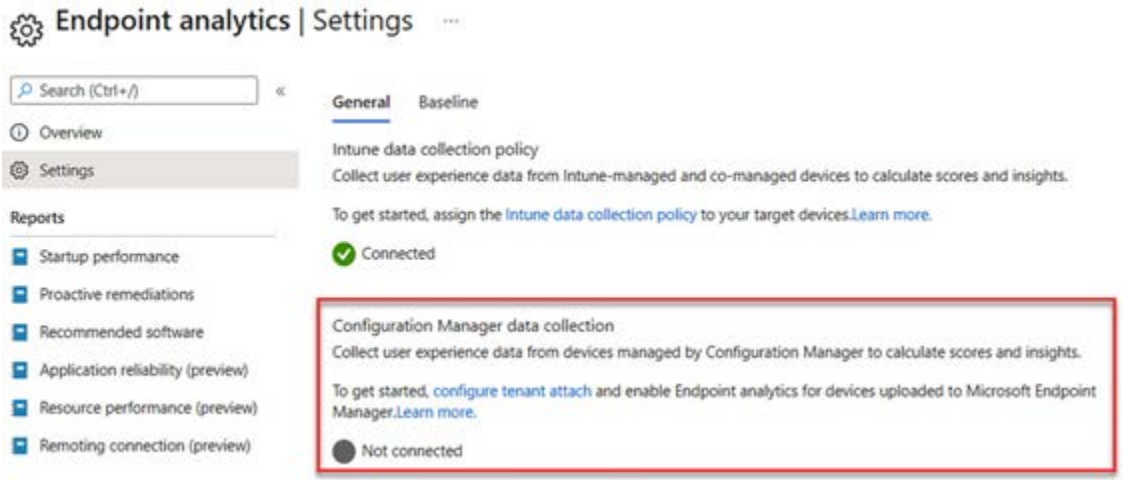


Figure 14.23: Settings menu

Customizing your baselines

Change your baselines to your own values via the **Settings** menu, as you could have higher or lower principles as the default settings. This will allow organizations to adjust the scorings to standards that match the expectations of their environment and applications.

Baselines define the score and whether indicators show up in green or red in Endpoint analytics. Be careful when defining your own baselines to ensure the quality and performance level of your Windows physical and cloud PCs.

You can see in the following screenshot how you can change the baseline regression thresholds. You can find this setting under **Endpoint analytics | Settings**.

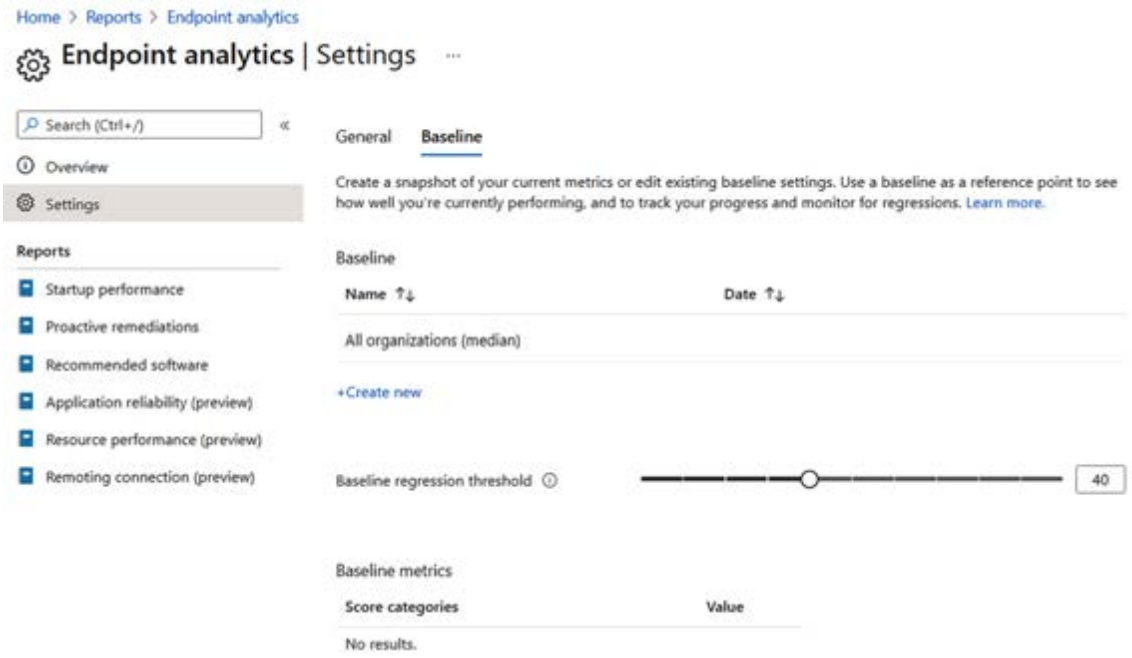


Figure 14.24: Changing the baselines

Remediations

Another great benefit of using Endpoint analytics is that you can create and run script packages on devices to proactively find and fix the top support issues in your organization.

For example, you can create detection scripts that search for settings on your Windows endpoint – if the setting or registry key no longer exists, it fires off the remediation script to get the setting back in. This is a very unique and proactive way to make sure that your environment remains consistent.

The section shown in the following screenshot allows you to see the status of your deployed script packages and monitor the detection and remediation results. Results are shown as the number of devices affected.

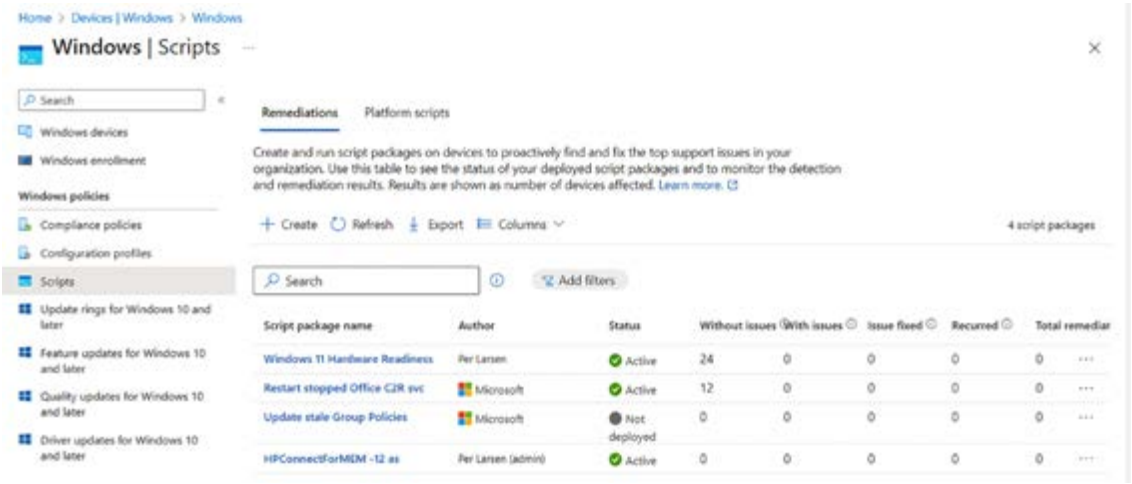


Figure 14.25: Remediation scripts

If you want to create a proactive remediation script package action yourself, you simply click on + **Create script package**.

Enter a name for the script and configure the detection and remediation script with the right settings, as in the following example in *Figure 14.26*.



NOTE

If you are adding registry keys to a 64-bit Windows endpoint, make sure to enable **Run script in 64-bit PowerShell** to ensure it is in the correct location!

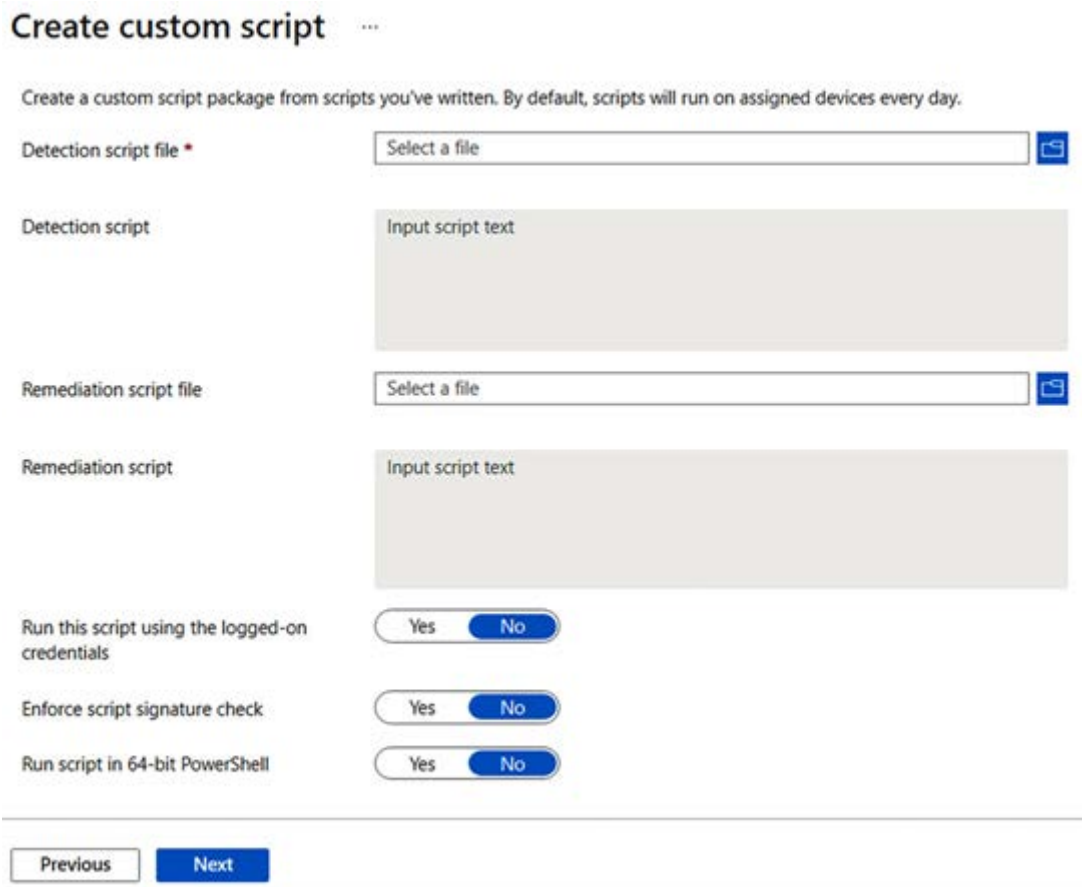


Figure 14.26: Create custom script

Assign the custom script actions to the right groups/users either via Entra ID or on a device basis and the detection will start directly:

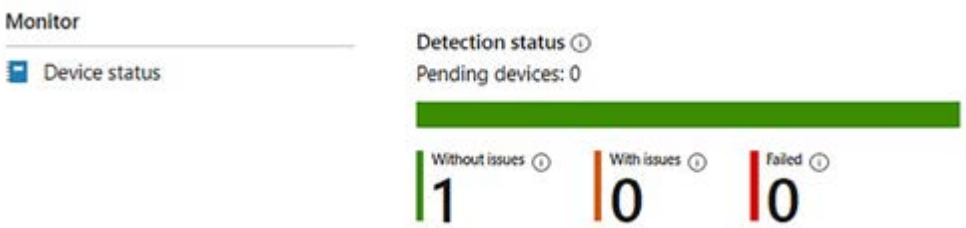


Figure 14.27: Detection status

You can also run a remediation script on-demand as a remote action from within:

1. Go to **Intune Admin Center | Device | Windows.**
2. Then search for the device and **Run remediation.**

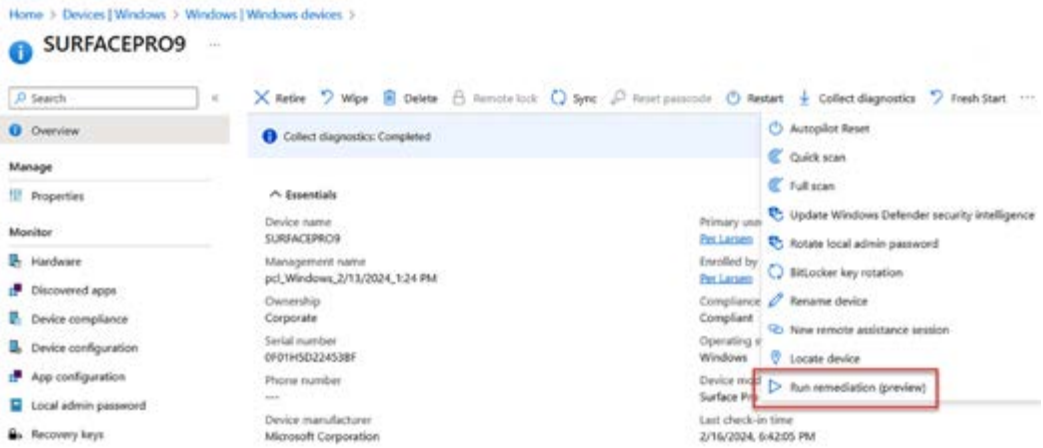


Figure 14.28: Run remediation on-demand

3. You will get a list of available remediation scripts and you can select the one that you want to run.
4. Click **Run remediation.**

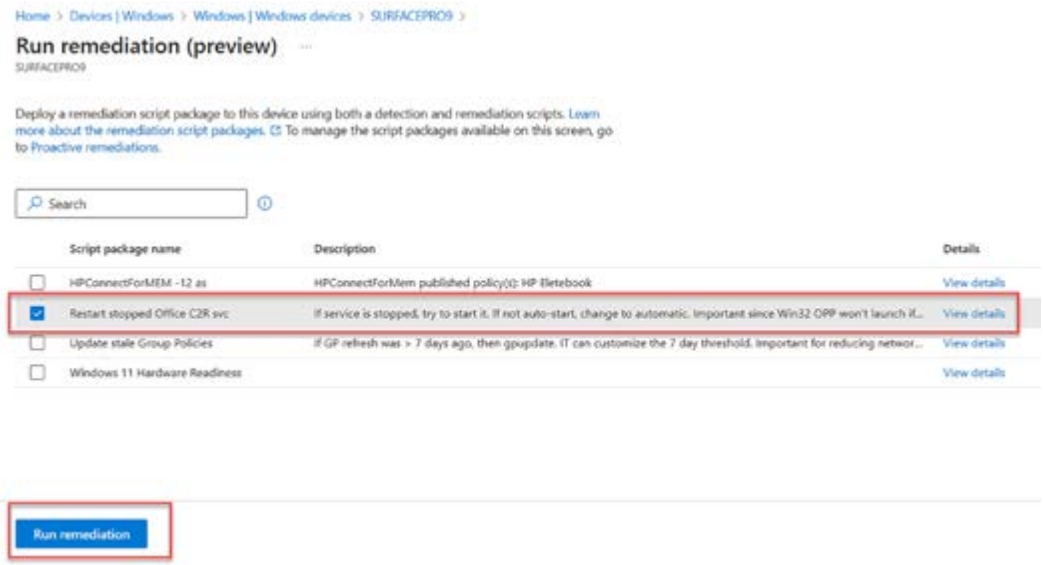


Figure 14.29: Run remediation script



NOTE

Remediation script on-demand is currently not available for Windows 365 devices managed by Intune.

You can find more examples of PowerShell scripts for Remediations in the Microsoft Intune documentation: `https://learn.microsoft.com/en-us/mem/intune/fundamentals/powershell-scripts-remediation`.

This concludes the section on remediation scripts. In the next section, we will cover Windows 365 Frontline.

Windows 365 Frontline

This report is a valuable tool for customers seeking to optimize costs. It allows them to track license usage trends over time, enabling them to plan and adjust the number of licenses needed to maintain access during periods of peak usage. Additionally, the report sends alerts to IT administrators when they are nearing or have hit the concurrency limit. This ensures efficient license management and cost-effectiveness.

You can find this new dashboard under **Devices** | **Overview**.

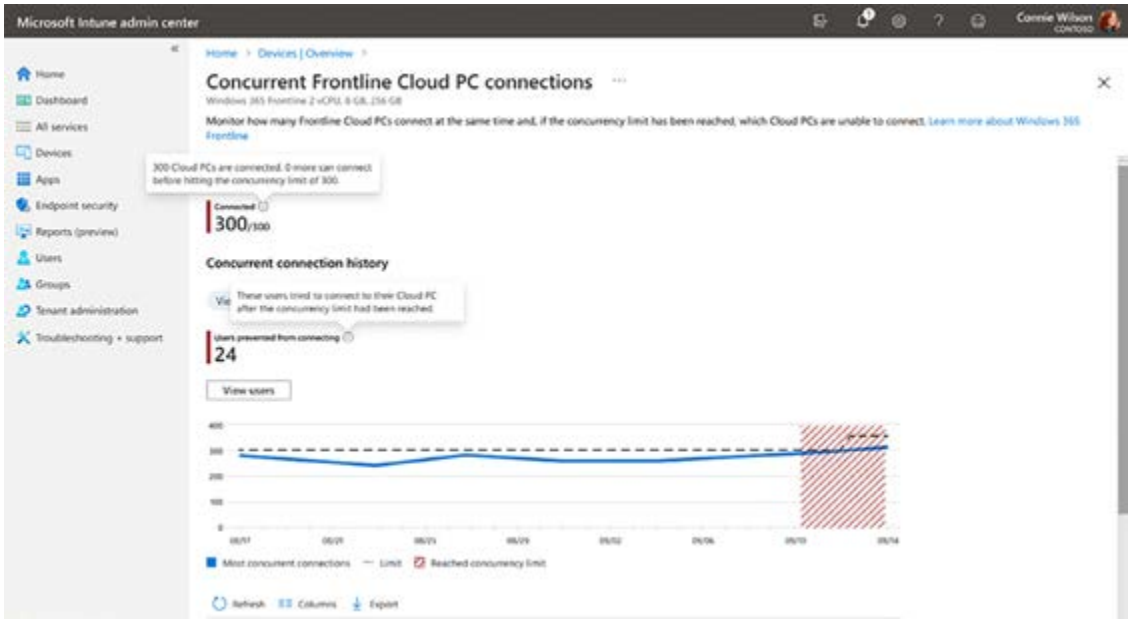


Figure 14.30: Concurrent Frontline Cloud PC connections

Azure Monitor integration

It's also possible to export diagnostics to Azure Monitor so you can query the data and do whatever you want with it. For example, you can create workbooks to map the status of your environment.

To enable this, you activate one of the diagnostic settings. There are also additional costs involved as it requires a storage account and a Log Analytics workspace.

The following list of logs can be automatically exported to a Log Analytics workspace:

- AuditLogs
- OperationalLogs
- DeviceComplianceOrg
- Devices

By enabling log analytics integration for Microsoft Intune in the diagnostic settings, as seen in the following screenshot, you will be able to create queries and a custom dashboard based on the telemetry data that is being collected in Azure Monitor:

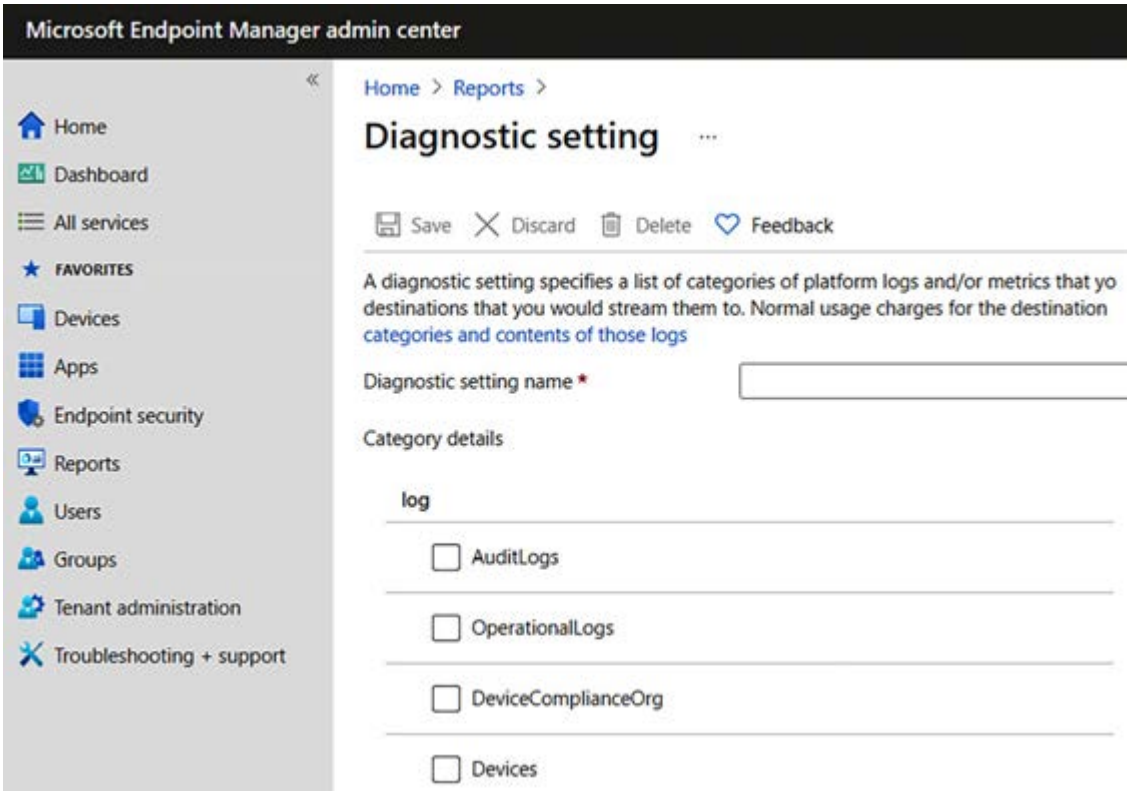


Figure 14.31: Diagnostic setting

System alerts and email notifications

Manually checking for failures in Microsoft Intune is not the most efficient workflow. Ideally, any failures or unexpected events should be automatically reported to you outside the system for quicker response times. This can be achieved with the integrated Alerts feature in Microsoft Intune. It allows IT Administrators to receive system notifications within the Intune portal and can be configured to send an email to one or more addresses – you can find how to do this in the next section.

Configure notifications for failed provisioning of cloud PCs

Configuring an alert in Microsoft Intune is easy and straightforward. We will show how to set up alert notifications if a cloud PC fails in the provisioning state. The process is similar if you want to have other alerts activated as well.

Start by going to **Microsoft Intune** | **Tenant Administration** | **Alerts**.

From here, select **Alert Rules** and choose **Provisioning failure impacting Cloud PCs**.

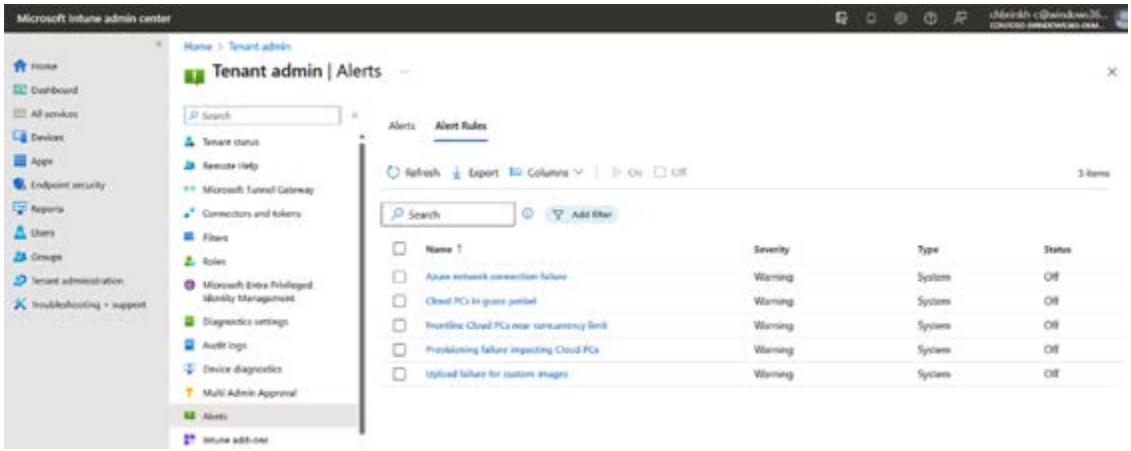


Figure 14.32: Overview of alerts rules

First, we need to define the conditions when the alert should be triggered. In this case, we want to get a notification whenever any cloud PC fails during provisioning. So, we set **Threshold** to greater than or equal to 1. Next, we can define what **Severity** the alerts should have. Make sure to set **Status** to **On**.

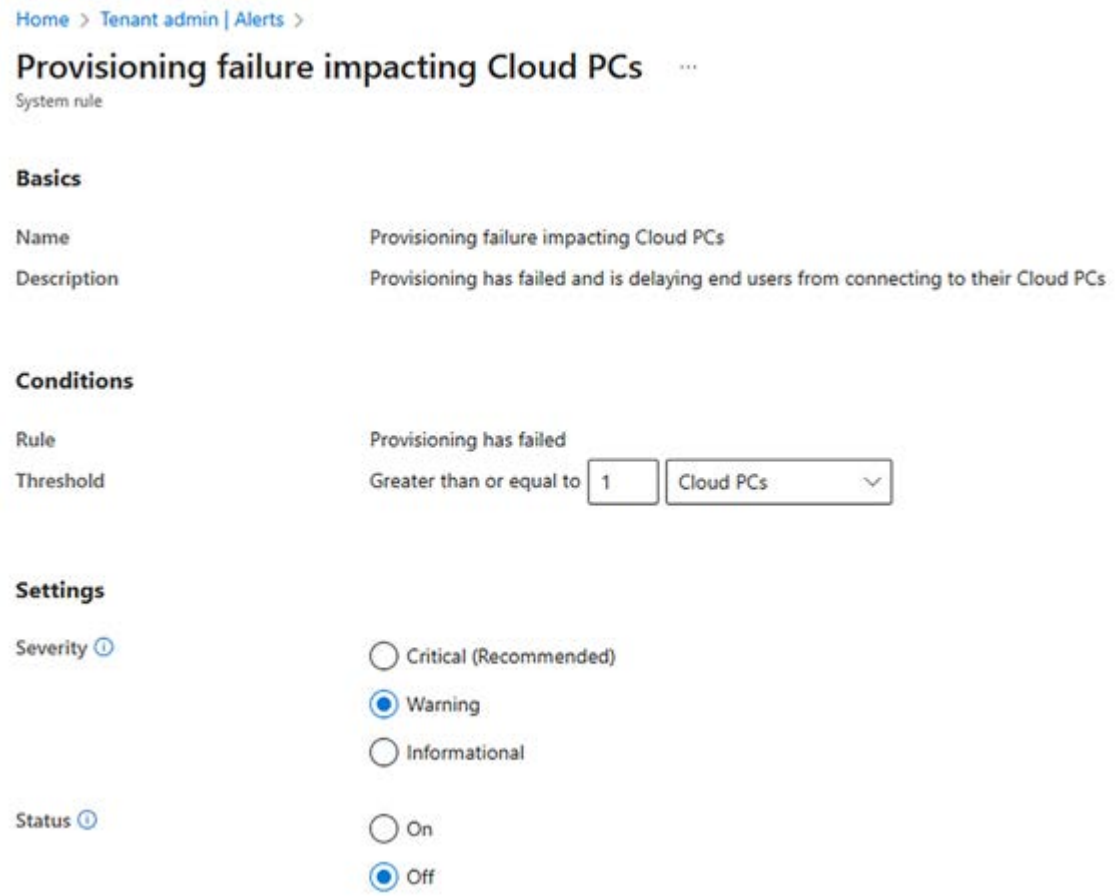


Figure 14.33: Configure provisioning failure alert settings

Now it's time to choose how we would like to get the notification. **Portal pop-up** will display a message in the Intune portal when you are logged in. **Email** will send an email to the addresses you specify in the language of your choice. Once done configuring the settings, select **Apply** and the alert rules will now be active.

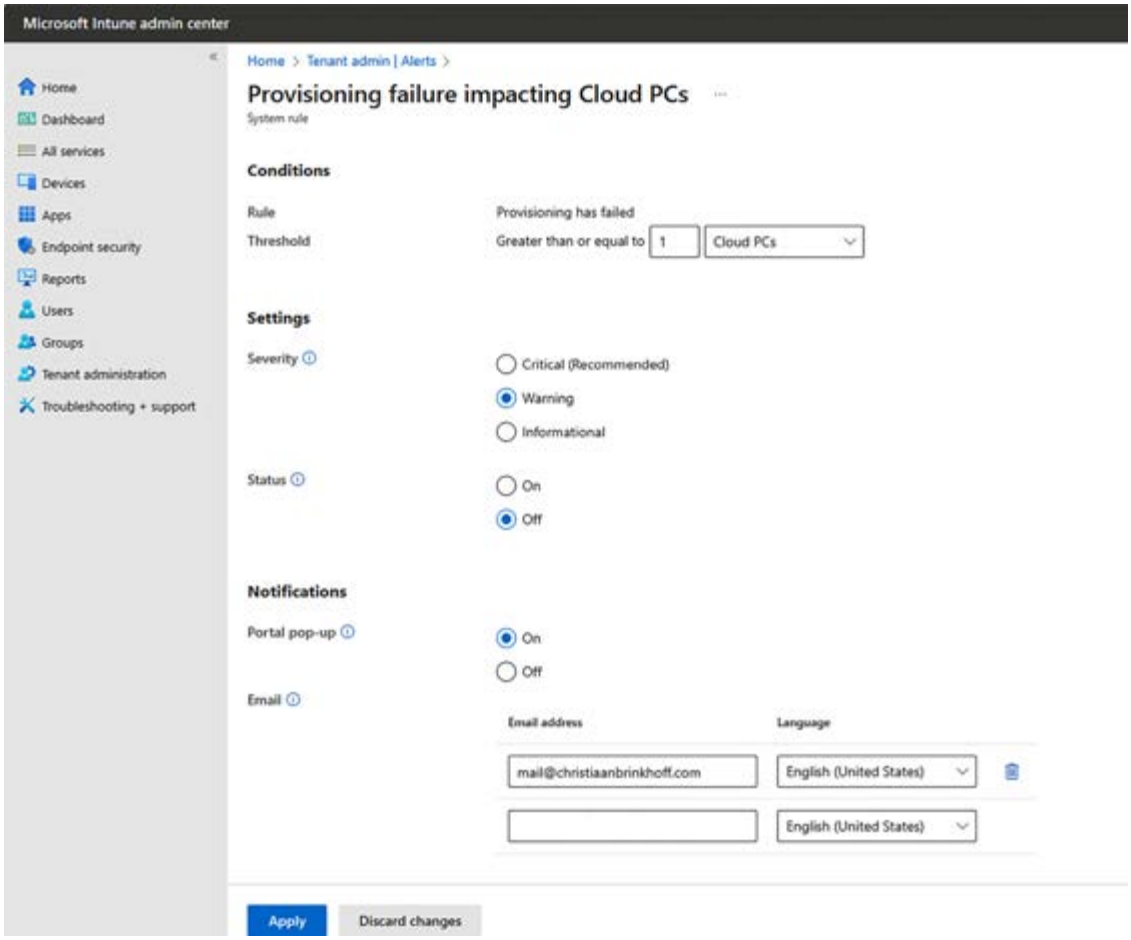


Figure 14.34: Configure notification for provisioning failure alert

You will be able to get an overview of all the triggered alerts by going to **Microsoft Intune Admin Center** | **Tenant Administration** | **Alerts**.

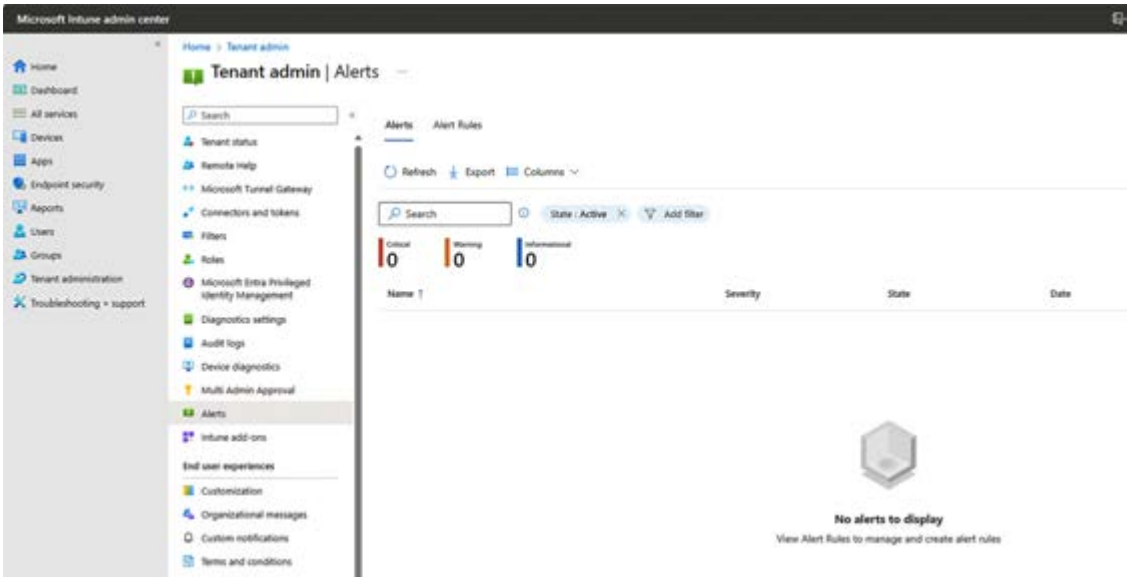


Figure 14.35: Overview of triggered alerts

Service health

As well as Endpoint analytics and the other monitoring capabilities explained in the previous section within Microsoft Intune, you can also monitor the service availability at a high level. If you experience issues or other problems within Windows 365, Microsoft 365, or Microsoft Intune, you can check the service health to determine whether it is a known issue with a resolution in progress before you call support or spend time troubleshooting.

To *find* the **Service health** dashboard, you must *open* the Microsoft 365 admin center portal.

Go to **Health** followed by **Service health**.

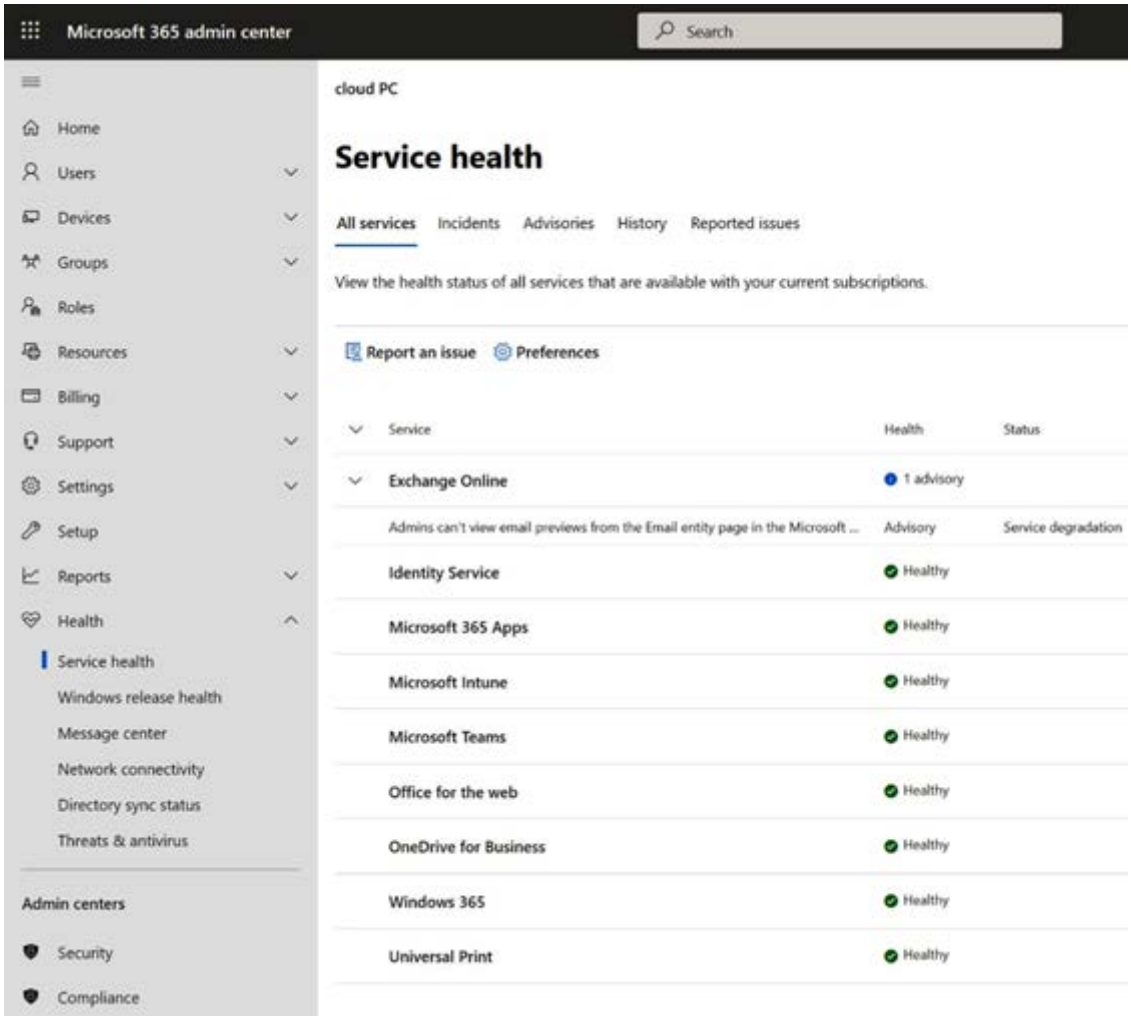


Figure 14.36: Service health

Let's talk a little bit more about going beyond the Microsoft Intune core features.

Advanced Endpoint analytics

Advanced Analytics is part of the Intune suite of Microsoft Intune. The advanced features of Endpoint analytics are seamlessly integrated into the existing base Endpoint analytics experience in the Intune admin center, under the **Reports | Endpoint analytics** section.

The new extra Endpoint analytics features are:

1. **Anomalies**: This feature can track the health of your organization's devices, looking for regressions in user experience and productivity following configuration changes. More information can be found in the **Anomaly detection** section.
2. **Scope tags**: This feature can be utilized to create custom device scopes, enabling you to tailor Endpoint analytics reports to a specific subset of devices. This allows you to view scores, insights, and recommendations that are specific to certain subsets of your enrolled devices. For instance, you can concentrate on devices under your management, devices allocated to a particular business group, or devices in a specific geographical area. More details can be found in the **Device scopes** section.
3. **Enhanced device timeline**: This feature provides more events and reduces data latency, aiding in the troubleshooting of device issues. More information can be found in the Enhanced **device timeline** section.

You will have read everything about Microsoft Intune Suite – Advanced Endpoint analytics in *Chapter 11*, *Intune Suite!*

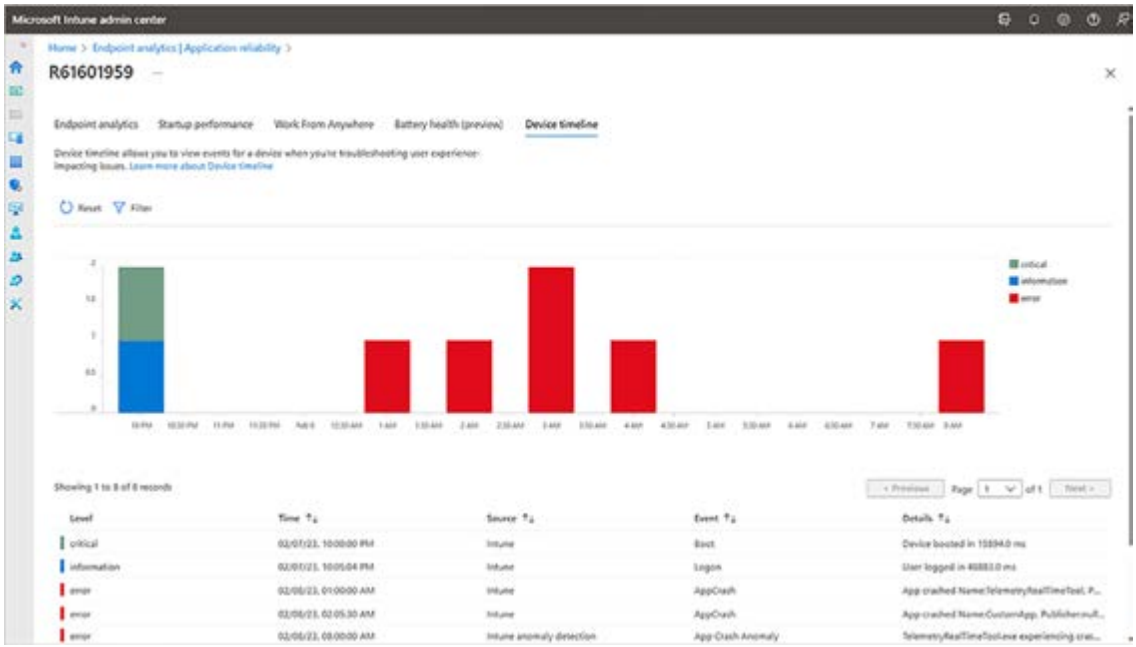


Figure 14.37: Application reliability

This concludes the chapter on monitoring and Endpoint analytics. As we have shown, you will only benefit from enabling Endpoint analytics in your environment to get more insight into your Windows estate.

ControlUp Enrich

We also have a broad partner ecosystem that can help you with monitoring both physical and cloud PCs, such as ControlUp Enrich.

ControlUp Enrich is available now in the Chrome and Microsoft Edge add-on stores and installation and setup takes only seconds. If you already have a ControlUp DEX environment, you are ready to go.

Learn more about it at: `https://www.controlup.com/resources/blog/entry/view-and-improve-device-digital-experience-from-inside-microsoft-intune-with-controlup-enrich/`.

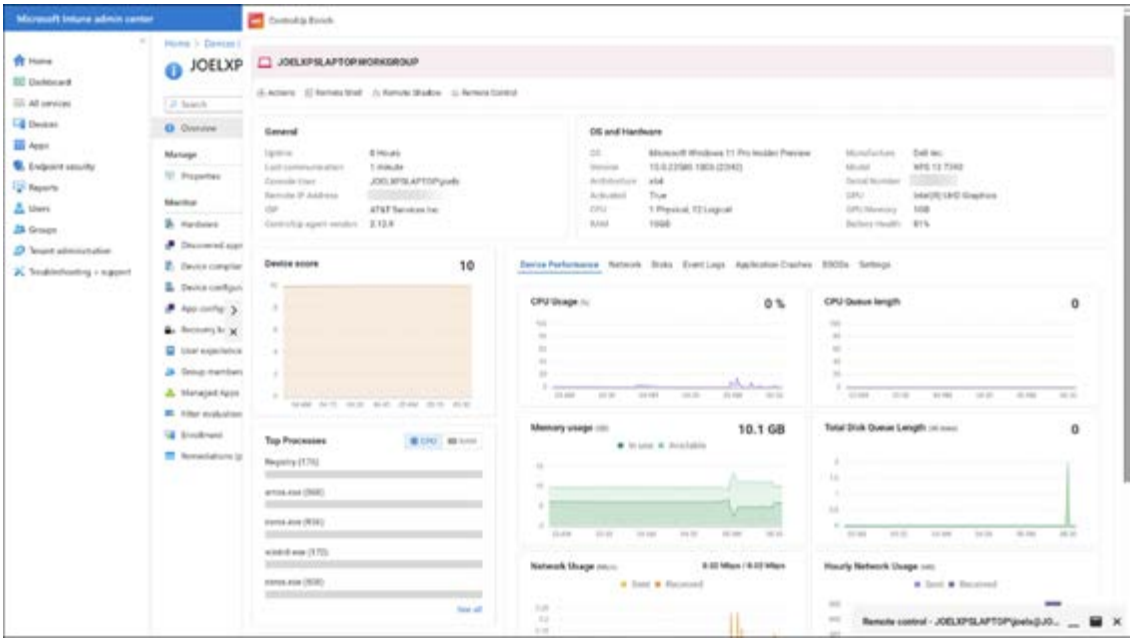


Figure 14.38: ControlUp Enrich

Summary

In this chapter, you've learned about the different monitoring, analytics, and reporting capabilities within Microsoft Intune. Endpoint analytics gives you great insights that you can react to, but remediation scripts provide the option to detect issues before the end user notices and remediate them. This is the best way to keep your end users productive and keep support calls to a minimum. Endpoint analytics is part of the Microsoft Intune and Windows Enterprise license, at no additional cost; you should just enable it to start getting data on your devices, which includes information on app crashes and reasons for reboots, including a blue screen. In addition, Advanced Endpoint analytics covers more advanced scenarios, and we covered that in *Chapter 11*, *Intune Suite*.

In the next chapter, we're going to explain to you how you can simplify your traditional printing environment with Microsoft Universal Print.

Questions

1. Is Advanced Endpoint analytics part of Intune Suite?
    a. Yes
    b. No
2. Is it possible to measure the logon duration of your physical and cloud PCs?
    a. Yes
    b. No
3. What does the service health dashboard show?
    a. The availability of the different Microsoft cloud services
    b. The SLA of the different Microsoft cloud services
    c. The downtime of the different Microsoft cloud services

Answers

1. (a)
2. (a)
3. (a)

Further reading

If you want to learn more about monitoring and analytics after reading this chapter, please use one of the following free online resources:

- *What is Endpoint analytics? Microsoft Intune | Microsoft Docs*: `https://docs.microsoft.com/en-us/mem/analytics/overview`

Join the CloudPro Newsletter with 44000+ Subscribers

Want to know what's happening in cloud computing, DevOps, IT administration, networking, and more? Scan the QR code to subscribe to **CloudPro**, our weekly newsletter for 44,000+ tech professionals who want to stay informed and ahead of the curve.



`https://packt.link/cloudpro`

15

Universal Print

Businesses are doing more and more things digitally; however, printing on physical paper remains important. Universal Print is a relatively new platform-as-a-service on Azure that can simplify the whole printing configuration and maintenance process compared to a traditional print server environment.

After reading this chapter, you will be able to connect both legacy printers and modern printers that are Universal Print ready to the Microsoft cloud. We'll also take a closer look at how you can assign printers to physical PCs and Cloud PCs as endpoints via Intune.

Long story short, you will become an expert in printing!

In this chapter, we'll go through the following topics:

- What is Universal Print?
- Is Universal Print secure and where does my printed data go?
- Universal Print – architecture overview
- Configuring Universal Print
- Print clients – Windows
- Print clients – macOS
- Printers – Universal Print ready printers
- Creating a printer share for a printer
- Testing your Universal Print printer and printer share
- Assigning and deploying cloud printers with Microsoft Intune

What is Universal Print?

Universal Print is a cloud-based print solution that allows IT admins to share printers as organizations migrate their users and devices to the cloud. Universal Print enhances security and privacy, reduces complexity for IT admins, and simplifies printing for end users. It eliminates on-premises print servers and lets you easily manage printers via a centralized portal in Azure. Admins can deploy printers on end user devices directly with Microsoft Intune.

Universal Print is built with the **Internet Printing Protocol** (**IPP**) standard. You can now say goodbye to installing (and maintaining) printer drivers on devices and/or base images. Also, everything works with **Microsoft Entra ID**. This means that users can use the same set of credentials they use for other Microsoft services, like Windows 365 and Office 365 for Web, to print documents directly from a web browser via Word!

Here are some key benefits of using Universal Print:

- It accelerates your migration from on-premises to the cloud.
- Simple and secure print deployment architecture for zero-trust environments.
- No print drivers on end user devices.
- No VPN for printing. Users can easily print from anywhere.
- Seamlessly print from anywhere with consistent experiences – Windows, Mac, and cloud applications (like OneDrive for Business and Microsoft Excel in a web browser).
- Print from custom **line-of-business** (**LOB**) applications with simple integrations using the Microsoft Graph API.
- Serverless deployments with Universal Print ready printers.

Your existing licensing most likely already includes the Universal Print licenses – most customers who are eligible to use Microsoft Intune also get Universal Print licenses. You can find the licensing requirements for Universal Print in the requirements section later in this chapter.

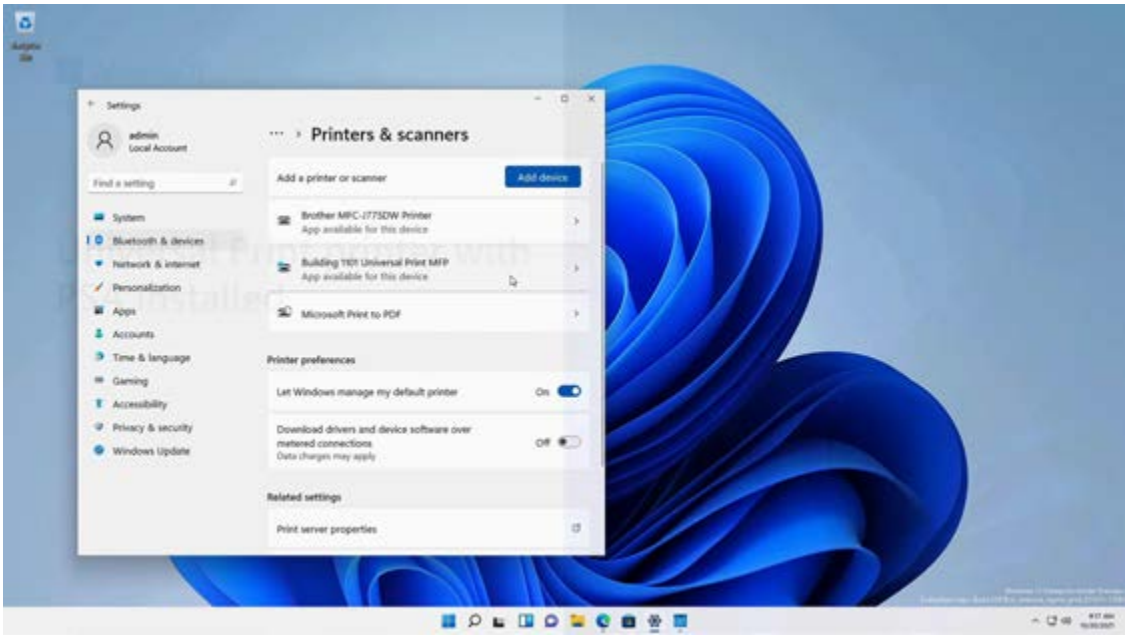


Figure 15.1: Windows 11 Printers & scanners

Universal Print – architecture overview

The core **Universal Print service** runs in the cloud as a platform on Azure. Users send print jobs to the service using different **clients** (like physical or virtualized Windows devices, Mac, cloud applications, etc.). Printers connect to Universal Print services and download submitted print jobs for printing.

Several printer models can communicate directly with Universal Print – these printers are called **Universal Print ready printers (more about them later)**. Universal Print ready printers provide the best Universal Print experience to both the admins and users.

Printers that lack the Universal Print ready support status to communicate directly can use the **Universal Print connector**. The connector can be installed on any host running Windows Server or the Windows client **operating system** (**OS**). The host machine needs to be on the same network as the printers. The connector host may be a physical device, virtualized on-premises, or hosted on Azure:

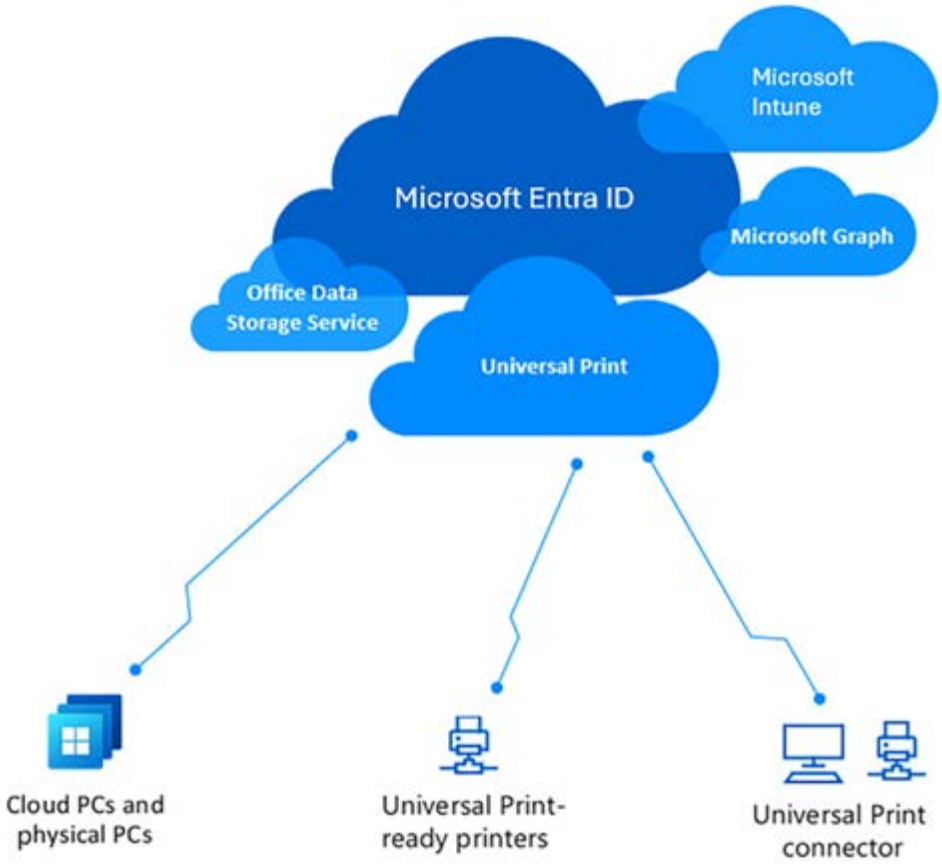


Figure 15.2: The architecture of Universal Print – used with permission from Microsoft

To use Universal Print, users and printers should be provisioned in the organization's Microsoft Entra ID (formerly known as Azure Active Directory) tenant. Printers are provisioned as devices in Microsoft Entra ID. Universal Print uses Microsoft Entra ID to authenticate each request from users and printers.

Universal Print uses Office storage for print queues and storing users' print data. Office storage refers to storage that is used by other Office products as well – for example, user mailboxes in Outlook.

Print clients – Universal Print for Windows

Windows users experience Universal Print printers like any other printer they print to. Users can print from any application on Windows and Universal Print printers are available across all types of print dialogs:

- Traditional print dialogs in apps like Notepad
- Modern print dialogs like the Microsoft Edge browser
- Custom print dialogs like Adobe Acrobat Reader or Microsoft Office applications

Windows integrates with Universal Print using the driverless IPP and makes printing independent of traditional printer drivers. This is especially powerful given the different platforms Windows supports – like x64, ARM, Windows 365, and **Azure Virtual Desktop** (**AVD**).

Universal Print uses **single sign-on** (**SSO**) on Windows. Users need to log in to their Windows device using either their Microsoft Entra ID identity or the hybrid identity using Microsoft Entra ID. Windows uses the user's logged-in identity to authenticate while communicating with the Universal Print service.

Also, something that is good to mention is that Universal Print supports most Windows platforms like x64, ARM, Windows 365, and AVD. Recently, Universal Print also added support for Windows 10 and Windows 11 multi-session.

Print clients – Universal Print for Mac

Great news: Universal Print now also works on macOS. Launched as a private preview in the later part of the calendar year 2023, this feature offers comprehensive support for Mac devices within the Universal Print framework. It enables users to print from any application using the Mac's built-in print dialog. Like Windows, it eliminates the need for driver installation on Mac as well.

Administrators can now proceed with confidence and adopt Universal Print in their environments with a mix of Windows and Mac devices, knowing that all their employees, irrespective of their OS, are supported.

The inclusion of support for Mac endpoints (Ventura 13.1 or later) and a user-friendly pull print function allows employees to print securely and conveniently on any company printer, from any location and device. Please read this document for any follow ups about Universal Print for macOS: `https://learn.microsoft.com/en-us/universal-print/macos/universal-print-macos-faq`.

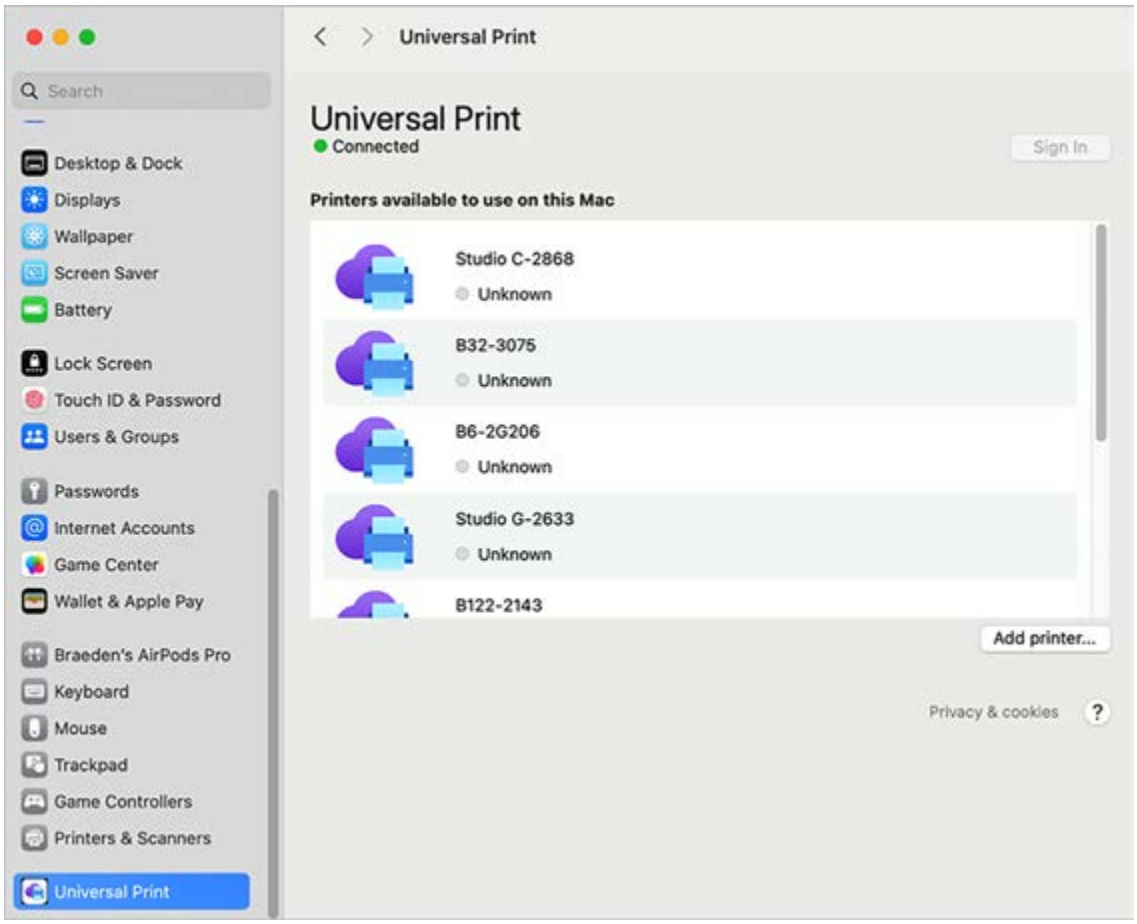


Figure 15.3: Universal Print – printers on Mac

Print clients – Web applications and print APIs

Web applications can easily integrate directly with Universal Print using the Microsoft Graph API. These applications bypass the print system of the underlying OS and make printing independent of any OS. This is especially powerful for cloud applications that may run on different platforms.

Microsoft leverages the Graph API to integrate printing from the browser experience of OneDrive for Business, Microsoft Excel, and Dynamics 365. More applications may be integrated in the future.

Printers – Universal Print ready printers

Before registering a printer with Universal Print, you should always check whether the printer model is Universal Print ready or not. Most printer brands already offer Universal Print ready printer models. In many cases, customers can either upgrade their printer firmware or install an application on the printer that will offer Universal Print ready functionality.

If your printer is Universal Print ready, you can then connect the printer directly to the cloud! There's no need for an ExpressRoute or a site-to-site VPN connection.

See the following example of a Lexmark Universal Print ready printer's web configuration page. Universal Print is listed as one of the network interfaces that can be used:

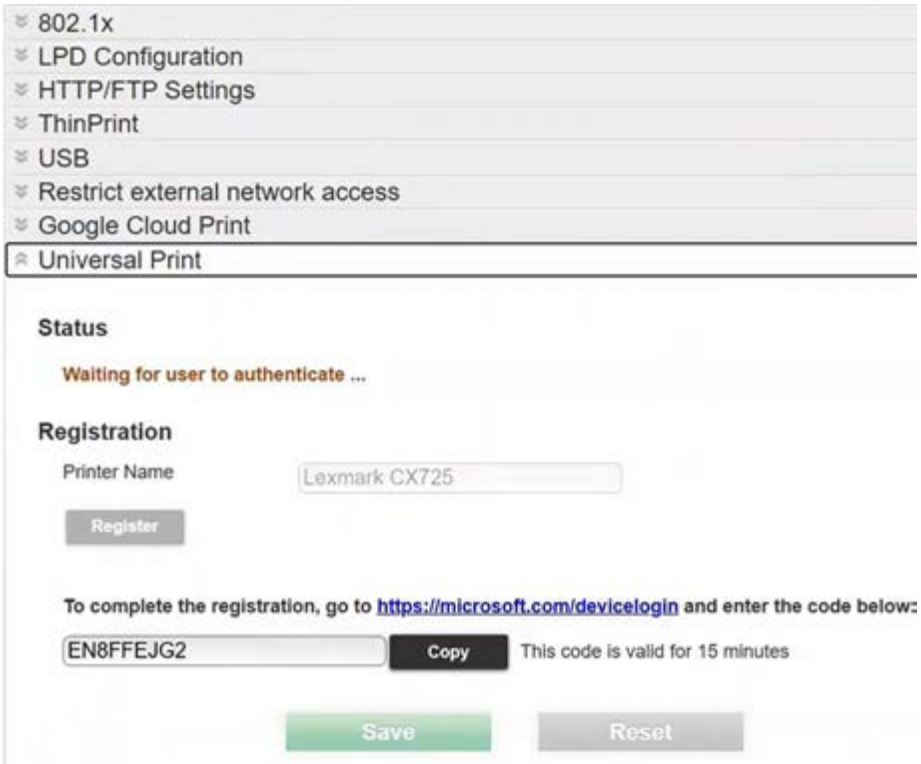


Figure 15.4: Universal Print – Lexmark printer settings

Universal Print ready printers can be deployed within the firewall of the organization. All connections to the Universal Print service are initiated by the printer itself. The communication channel between the service and printer is encrypted using HTTPS/TLS.

With traditional printer driver interfaces, printers supported a wide range of print options and customized workflows – especially with Windows. Most print options, including finishing options like stapling, hole-punch, and binding, are available through the IPP, and Universal Print ready printers can directly declare these options with Universal Print.

One of the great features available through the IPP is the PIN protection of print jobs. When a printer indicates its support for PIN release via the IPP list of options, a print dialog will allow users to create a PIN.

These jobs are sent to the printer, but they wait for the user to show up at the printer, select the print job, and then enter the same PIN before the job gets printed. This provides a basic level of privacy to the user and security for confidential documents. As per the current documentation, Epson, Lexmark, and Sharp provide PIN release with their Universal Print ready printer models. The partner integration page will be updated as new information becomes available.

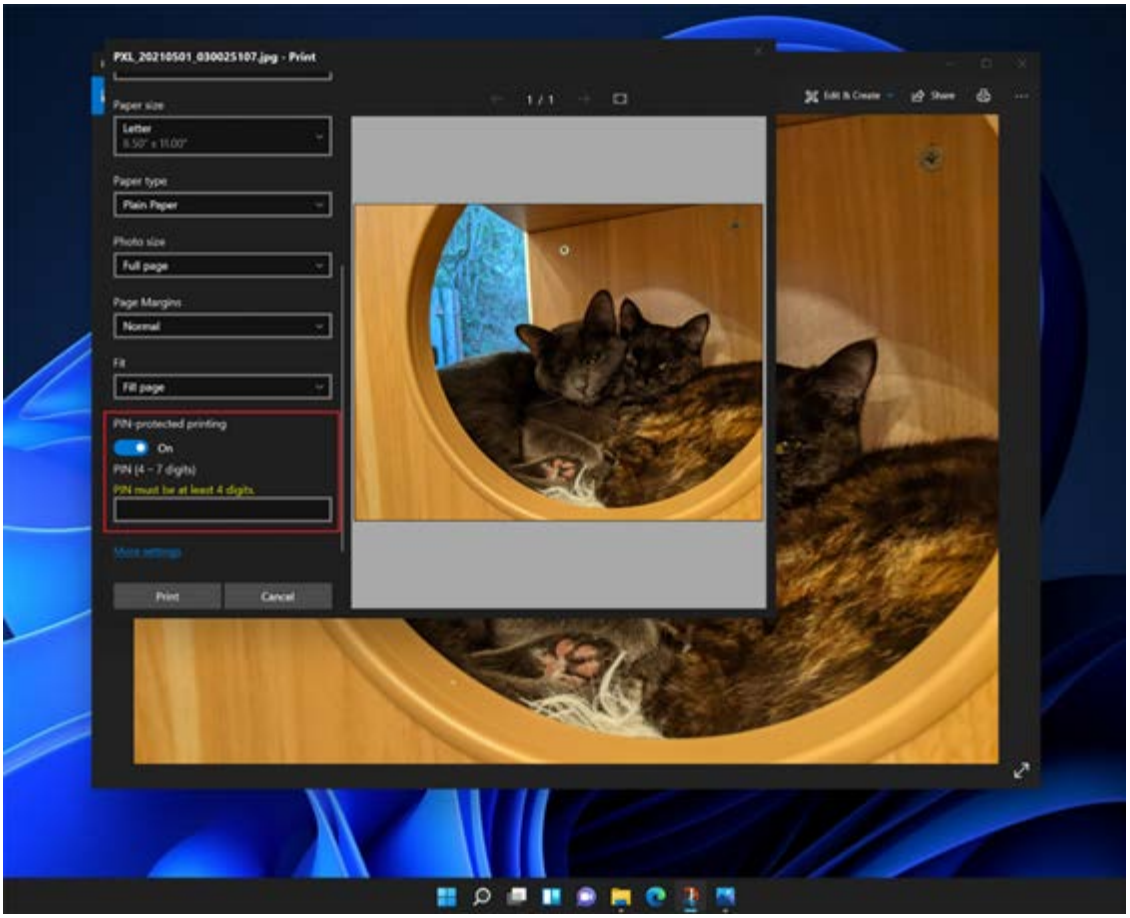


Figure 15.5: Universal Print – Windows print dialog with PIN

Later in this chapter, we will talk about the advanced secure release options that Universal Print provides. Universal Print ready printers may leverage the same secure release platform and offer even more options like badge-swipe.

To support more proprietary print options and workflows, printers can publish a **print support application** (**PSA**) on Windows. A PSA gets mapped to the printer on the user's Windows device.

A PSA may enhance the print experience in the following ways:

- It provides a custom user interface under the Advanced Printer properties of a print dialog on Windows. The custom interface may list standard IPP options as well as customer options.

This experience takes over the default experience in Windows for advanced print options.

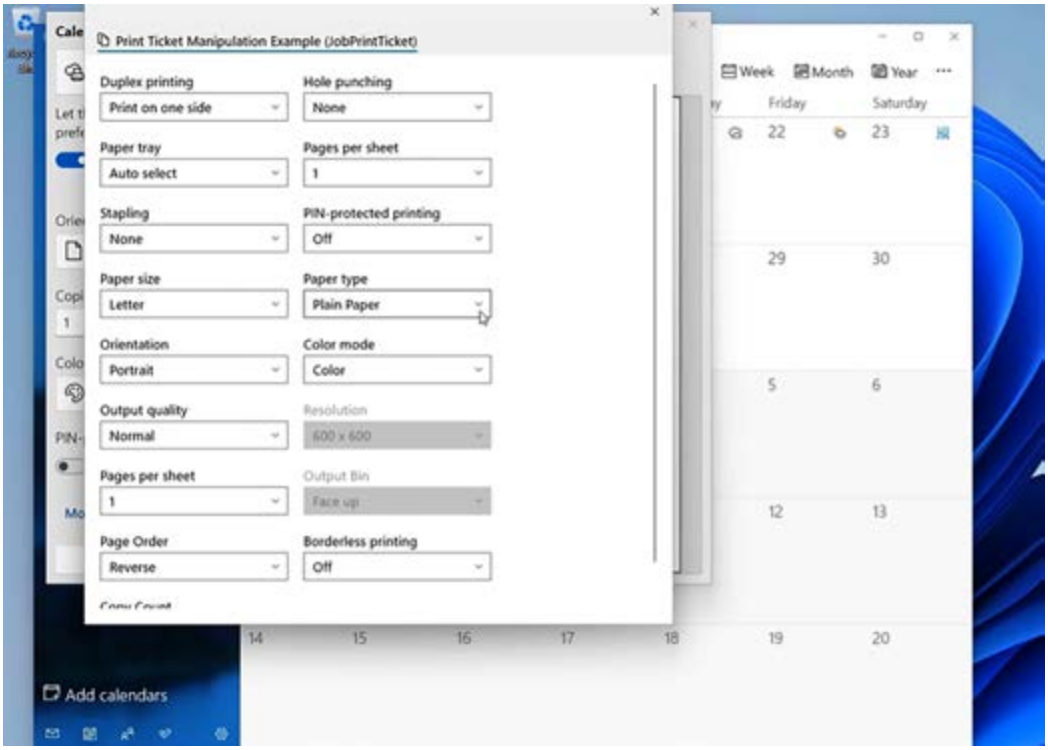


Figure 15.6: Universal Print – PSA in Windows

- After the user clicks **Print** action in the **Print** dialog, it may run in the background or invoke an additional print experience (e.g., trigger a custom workflow to enforce a print policy like mandating a user PIN).



When a printer declares a print option as per the IPP standard, it is available across any client that integrates with Universal Print. On the other hand, print options and workflows that are customized through PSA will be available only on Windows devices.

Printers – Universal Print connector

While there are Universal Print ready printer models in the market, many organizations will have printers that were procured a long time ago. These printers may not have any updates from the manufacturers to upgrade them to Universal Print ready. These printers can work with Universal Print using the Universal Print connector.

The connector software can be installed on either a Windows Server or Windows client host. It can be thought of as a proxy that sits between the printers and Universal Print service over the internet to follow the same zero-trust model as Universal Print ready printers. If you allow access to the URLs provided earlier in this chapter, you are all set. Say goodbye to **virtual local area network** (**VLAN**) management!

Here are some important things to keep in mind:

- Printers are installed on the connector host using manufacturer print drivers.
- There needs to be a direct network between printers and the connector host. The connector host may be deployed on a physical device or on an on-premises **virtual machine** (**VM**) that is within the same network as printers. It may also be deployed as an Azure VM with an ExpressRoute or a site-to-site VPN connection with the printer network.

See the following Universal Print connector connection process. We'll explain more about this process later in this chapter:



Figure 15.7: Universal Print – Connector registration

After printers are registered with Universal Print, administrators need to take a few more steps to make them available to users for printing.

Printer shares

Administrators need to create printer shares for registered printers. End users will always see printer shares and do not have direct visibility of printers. Admins can set up access controls on printer shares to restrict access to print to only a certain amount of users. For example, only the users in the HR department can print to printer shares for printers on the HR floor.

Users may either manually find and use printer shares, or admins can assign printer shares to users' virtual (and physical) Windows desktops using Microsoft Intune.

Printer defaults

All the management of Universal Print happens from within the Azure portal, and this also applies to changing the printer's default settings, such as color mode, two-sided print, and so on. Normally, you would have logged on to a traditional print server; with Universal Print, you can do it from the cloud from one management console (see the following example).

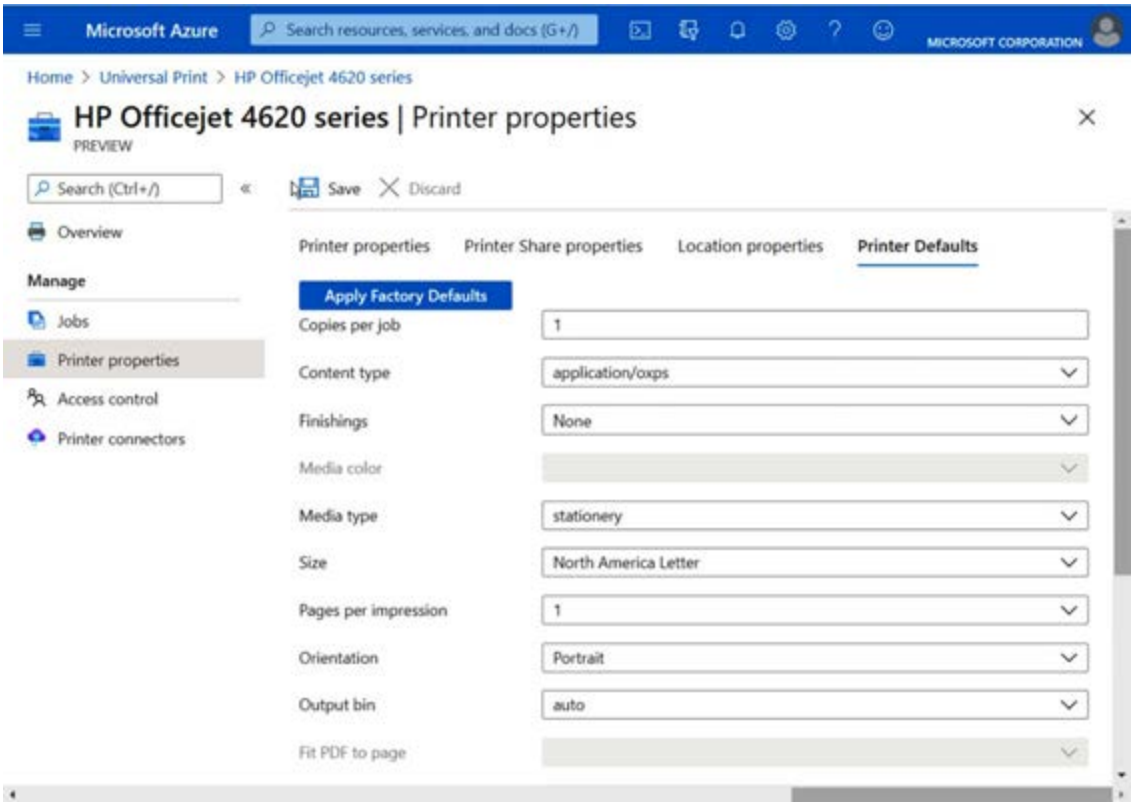


Figure 15.8: Universal Print – printer defaults

The defaults that administrators define are automatically taken over by the printer on Windows 10 and Windows 11 physical or Windows 365 Cloud PCs when a printer is added to the user's device. If a user does not modify the print options while printing, the default options will be used.

Is Universal Print secure and where does my printed data go?

With Universal Print, the print data goes via the cloud. This is very similar to the way other Microsoft enterprise technologies like Outlook, OneDrive for Business, and Microsoft Teams upload data in the cloud. All print data is stored in Office data storage like other Office technologies.

Universal Print stores data as follows:

- There is a storage provisioned for each user in Office storage – just like Outlook provisions a mailbox. The documents that the user prints are uploaded in Universal Print and stored in this user's storage.
- Each printer has its own storage provisioned in Office storage too. The printer's storage stores all the printer metadata and print queues. The print queues store only the print job metadata as the documents are stored in the user's storage.
- Universal Print also provisions some metadata, like a list of printer shares in Azure. This information is used to speed up operations like finding specific printer shares.

All data for a given print job stays in Universal Print only for a few days. If a job is not claimed at the printer within three days of the time of submission, it gets marked as aborted. Even after printing, a job may stay in Universal Print for a few more days (up to a total of 10 days from the time of submission). To cancel one or more print jobs, select the jobs and click **Cancel** in the command bar at the top of the **Jobs** list.



Print jobs cannot be canceled if they are in one of the final states – **Completed**, **Canceled**, or **Aborted**.

In the next section, you will learn more about where the print jobs are redirected and processed.

Data Residency

Universal Print processes all customer data in the geography the customer's tenant was created in. Print documents are stored in the storage provisioned for each user. The user's storage is provisioned in Office storage as per the Data Residency policies configured by the customer. Universal Print stores all customer data in the geography the customer's tenant was created in. Customer data is not stored or moved outside the tenant's geography. For example, if the customer has a tenant created in the US but has offices globally with preferred data locations set up in different geographies, then data will be handled as follows:

- All print requests will be redirected and processed in the US.
- All printer metadata and data stored in Azure will be stored in the Azure data center closest to the customer's tenant country. In this case, it will be the US.
- All print documents will be stored in the user's storage, which will be configured as per the user's preferred data location. If a user's location is India and that is set as their preferred data location, then their print documents will be stored in India.

To dive deeper into the different sets of privacy controls for printer jobs data management, please take a look at this documentation article: `https://learn.microsoft.com/en-us/universal-print/fundamentals/user-privacy-personal-data`.

Now, we are going to dive deep into the world of data security and printing with Universal Print.

Data security

All connections to Universal Print are first authenticated. User-initiated requests to Universal Print (like submitting a print job) use the user's Entra ID token. Similarly, printers and connectors use the device token. The device token is generated using the certificate that Entra ID provides at each printer registration. If there are cloud applications that use the Microsoft Graph API, they can use the application token to authenticate into Universal Print.

Data is encrypted in transit (over the network) and at rest (non-volatile storage), giving customers end-to-end encryption.

In transit, encryption is "on" by default and there are no controls to turn it off. Universal Print uses HTTPS and TLS with AES-256 encryption in all regions. All internet traffic is handled via **Azure Front Door** (**AFD**). For more information on how encryption in transit is handled, refer to the documentation of *AFD*.

At rest, since Universal Print uses Office storage, data is handled in the same way as other Office applications. By default, **Microsoft-managed keys** (**MMKs**) are used. Customers can use **customer-managed keys** (**CMKs**) if desired. For more information, search online for Microsoft 365 Data Residency.

Now, let's learn more about the different security certifications Universal Print offers for compliance.

Compliance and certifications

Universal Print has the following security certifications:

- HITRUST
- ISO 27017
- ISO 27001/2
- ISO 27018

For US government clouds, Universal Print has FedRAMP certifications. Universal Print complies with all laws and is **General Data Protection Regulation** (**GDPR**) compliant.

In the next section, we will explain how you can check access to your printer shares.

Printer share access check

As mentioned earlier, administrators can set up user-level access for printer shares. Users do not have direct visibility to printers. They can access and print to only printer shares.

At the time of finding printer shares, Universal Print returns only the printer shares that a user has access to. Similarly, every time a user prints, Universal Print checks if the user still has access to the corresponding printer share.

For checking access at a printer share level, Universal Print checks if a user is a member of the Microsoft Entra ID security group that can be mapped to the given printer share.

Now, we're going to explain how you can configure secure print jobs with Universal Print.

Secure release

After a user prints to a given printer share, the printer may immediately start printing, or it may wait for user input on the printer. With immediate printing, there is a risk to confidential documents and user privacy.

For making the printer wait until the user is at the printer, Universal Print offers multiple secure release options:

- **User PIN:** This was discussed earlier in the chapter with Universal Print ready printers.
- **Badge/biometric/login**: This is one of the most commonly used types of secure release in which a user may indicate their presence at the printer by providing some identification (like a badge) or authenticating with their login credentials. This has different options:
    - **Job downloaded on printer storage**: The printer may download the print job along with the document to be printed from Universal Print and store it on the printer's storage. It is only when the specific user's presence is confirmed at the printer that the printer will process the job further.
- **Through third-party print vendors**: Several print vendors, like PaperCut and YSoft, have integrated their solutions with Universal Print, and these solutions offer secure release. For specific information, click on the *Learn more* link next to the toggle or refer to the Universal Print online documentation.

    For printers registered with Universal Print connector, some printer and third-party vendor print solutions may work. This may need additional configuration on the connector host. Turn on the **Enable hybrid AD configuration** toggle in the connector interface.

- **Scanning QR code with a mobile phone:** Universal Print offers a secure release solution where users can use their mobile phone camera to scan a QR code on the printer and log in to the Microsoft 365 phone app. They can then see their waiting jobs for the corresponding printer on the app and decide to release those jobs using their phone. Here are screenshots of the user's experience:



Figure 15.9: Universal Print – secure release using mobile phone

Now, we are going to dive deep into the requirements of Universal Print.

Universal Print – requirements

In this section, you will learn about all the prerequisites to use Universal Print.

End user requirements

End users must have the following to be able to search printer shares and print:

- A Universal Print-eligible Microsoft 365 or Windows SKU license. Alternatively, a user may have a Universal Print standalone license, meaning a license bought just for Universal Print versus a bundle license such as Microsoft 365 E3. Licenses for Universal Print are automatically distributed via Entra ID.
- Windows desktops that are:
    - Running Windows 11, or Windows 10 version 1903 onwards.
    - Joined to Microsoft Entra ID. Microsoft Entra Hybrid joined physical and virtual desktops are also supported.
- Alternatively, users can print from a Mac or cloud application that integrates with Universal Print (e.g., Microsoft Excel in a browser).

Admin requirements for managing Universal Print

Managing print requirements

To configure and manage Universal Print:

- Administrators should have either the Printer Administrator Entra ID role or should just be the Global Administrator.
- The printer technician Entra ID role allows only the registration of printers.
- A Universal Print-eligible license.
- An administrator may be a delegated admin assigned to one or more administrative units in Microsoft Entra ID. Delegated administrators can manage only the printers that are contained within their administrative units.

Here is a screenshot from the Admin Center portal with roles for Universal Print:

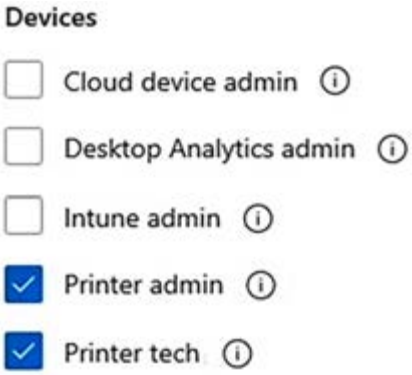


Figure 15.10: Universal Print role-based access controls

Universal Print – requirements

To use printers within Universal Print, Universal Print ready printers are preferred. These printers can connect directly to the cloud – without a Universal Print connector as software in between.

If you are using a Universal Print connector, then there are additional requirements for the connector host:

- The OS needs to be either:
    - Windows Server 2016 64-bit or later (Windows Server 2022 64-bit or later is recommended)
    - Windows 10 64-bit, Pro or Enterprise, version 1809 or later
- .NET Framework 4.7.2 or later
- Running 24x7 (e.g. sleep/Hibernate are disabled)
- Always has a connection to the internet
- Has access to all the internet endpoints mentioned in the **Network requirements** section

The memory and CPU on the connector host may vary depending on the number of printers it hosts and the collective print load on those printers. For example, Microsoft performed stress tests with no issues for 600 printers on a single connector host running as an Azure VM with 2 CPUs and 16 GB RAM.

After these more functional and licensing requirements, let's look at the network requirements. As Universal Print is a cloud service, you can imagine that a network and firewall are very important.

Network requirements

All devices that connect to Universal Print service (connector hosts and end user desktops) should be able to connect to the following internet URLs.

The following are the URLs that enable users to ensure successful printing via Universal Print in various scenarios.

Commercial cloud

Print service (printing)	`https://print.print.microsoft.com/`
Registration service (registering printers)	`https://register.print.microsoft.com/`
Discovery service (finding printer shares)	`https://discovery.print.microsoft.com/`
Notification service (notifying printer for waiting jobs)	`https://notification.print.microsoft.com/`
Graph service (cloud applications calling APIs)	`https://graph.print.microsoft.com/`
Microsoft Entra ID	`https://login.microsoftonline.com/` `https://azure.microsoft.com/en-in/products/cdn`
Documentation links	`https://go.microsoft.com` `https://aka.ms`

US government GCC cloud

Government Community Cloud (**GCC**) uses commercial cloud endpoints and the following URLs:

Print service	`https://gcc-print.print.azure.us/`
Registration service	`https://gcc-register.print.azure.us/`
Discovery service	`https://gcc-discovery.print.azure.us/`
Notification service	`https://gcc-notification.print.azure.us/`
Graph service	`https://gcc-graph.print.azure.us/`

US government GCC-High cloud

Print service	`https://print.print.azure.us/`
Registration service	`https://register.print.azure.us/`
Discovery service	`https://discovery.print.azure.us/`
Notification service	`https://notification.print.azure.us/`
Graph service	`https://graph.print.azure.us/`
Microsoft Entra ID	`https://login.microsoftonline.us/`

Network isolation and zero-trust

- `*.microsoftonline.com`
- `*.azure.com`
- `*.msftauth.net`
- `go.microsoft.com`
- `aka.ms`

For Microsoft's US-government-specific clouds (GCC and GCC High), the following URLs should also be reachable:

- `https://*.print.azure.us/`
- `https://login.microsoftonline.us/`

Universal Print allows customers to isolate the network of their end users from the network of their printer devices without needing any VPN. Network isolation can enhance security, and vulnerabilities due to unauthenticated access to resources on the same network can be avoided. Furthermore, with Universal Print ready printers, organizations can simplify deployment architecture and move Universal Print to a fully zero-trust environment. This reduces the surface area for unauthorized network attacks via Universal Print infrastructure.

Enough talking. Let's switch over to the deployment steps to deploy Universal Print in your environment.

Learning how to deploy Universal Print

Before we start, make sure that your environment uses Microsoft Entra ID – either fully cloud-managed or hybrid identity with Microsoft Entra ID. Make sure the **Windows 10 or later domain-joined devices** box has been ticked. You can find information about how to set up Entra ID join and Hybrid Entra ID join in *Chapter 13, Identity and Security Management*.

Also, make sure your users and administrators have an eligible Universal Print license assigned in your Entra ID tenant.

See the following screenshot to see how you can change your Entra ID Connect configuration to Hybrid Entra ID join during the setup flow:

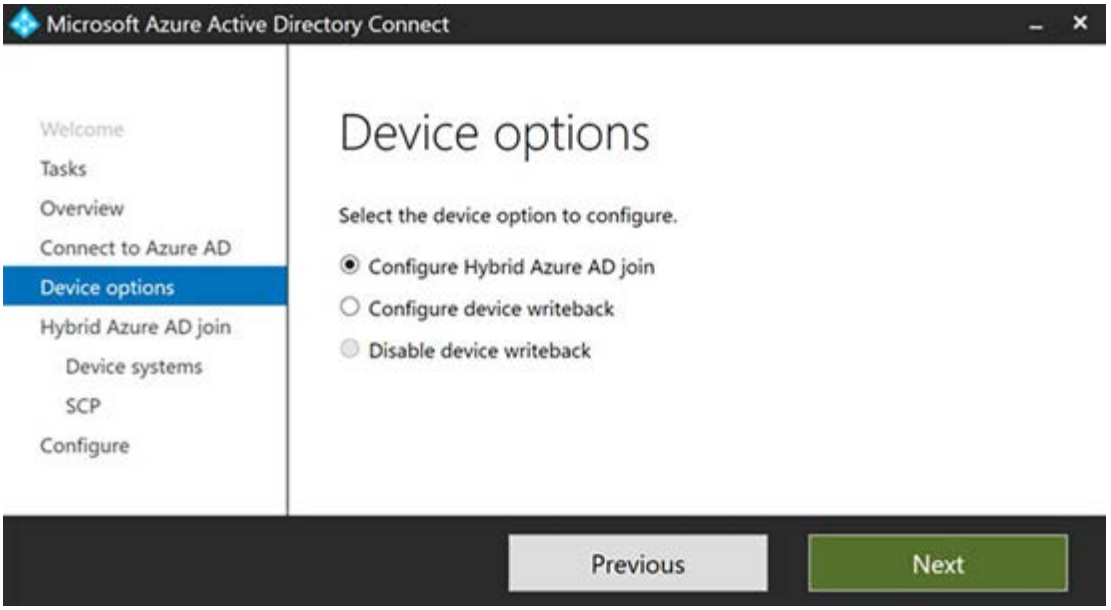


Figure 15.11: Entra ID Connect – enable Hybrid Entra ID join

Now, let's look at what rights you need to configure and maintain Universal Print.

Printer management — custom roles

Universal Print integrates with Microsoft Entra ID. Using Entra ID, you can designate limited privilege administrators to manage Universal Print. This allows you to configure and manage Universal Print with an account other than the Global Administrator.

Role Name	Role Description
Printer Administrator	Users in this role have full access to manage all aspects of printers in Universal Print.
Printer Technician	Users in this role can register and un-register printers and set printer status.

Table 15.1: Universal Print roles

Roles can be configured by Privileged Role Administrators or Global Administrators. To configure a role, go to Microsoft Entra Admin Center and then navigate to **Roles & admins** section under **Identity**.

Print management scope can be further restricted by using delegated administration and Admin Centerdministrative units in Entra ID. Printer administrators assigned to specific administrative units can manage only the printers within their administrative units. You may refer to the Universal Print online documentation on delegate administration for more details on this topic: `https://learn.microsoft.com/en-us/universal-print/`.

Now, you've learned about role-based access delegation. Of course, Microsoft isn't doing Universal Print all alone, and some features require partners to jump in. In the next section, you will find more information about this.

Connecting your existing printer to Universal Print

The following steps explain how you can connect your own printer to Universal Print. If your printer is Universal Print ready, you can skip the connector installation and connect to the Universal Print service directly from the printer over the internet.

The following steps explain how you can connect your own printer to Universal Print.

If your printer is Universal Print ready, you can skip the connector installation and connect to the Universal Print service directly from the printer over the internet. Here's a list of **original equipment manufacturers** (**OEM**s) that offer Universal Print ready printer models:

- Brother
- Canon
- Epson
- Fujifilm
- HP (with the HP Workpath app)
- Konica Minolta
- Kyocera
- Lexmark
- Ricoh (with a printer app)
- Sharp
- Toshiba Tec
- Triumph-Adler
- Xerox

The following cloud solutions also integrate with Universal Print:

- Konica Minolta Workplace Pure
- Konica Minolta Dispatcher Paragon
- Lexmark Cloud Services
- Printix SaaS
- Ringdale FollowMe
- uniFLOW Online
- Xerox Workplace Cloud
- Y Soft SAFEQ Cloud

Other solutions that integrate with Universal Print are:

- Celiveo 365
- ezeep Hub by ThinPrint
- Gespage
- Kofax ControlSuite
- MPS Monitor
- MyQ
- PaperCut
- Pharos Cloud
- PriApps
- Process Fusion UniPrint InfinityCloud
- Y Soft OMNI Bridge
- Y Soft SAFEQ on-premises

More information about the value-adding solution briefs and contact details can be found here: `https://aka.ms/UPintegrations`.

Let's jump into the configuration flow of Universal Print.

Configuring Universal Print

In this section, we explain everything you need to know to purchase licenses and configure and assign Universal Print printers to your end users. Let's start.

Log in to the Universal Print admin portal

1. Go to the Azure portal via `portal.azure.com` and log in with an account that has either the Print Administrator or a Global Administrator role.
2. Search for **Universal Print**:

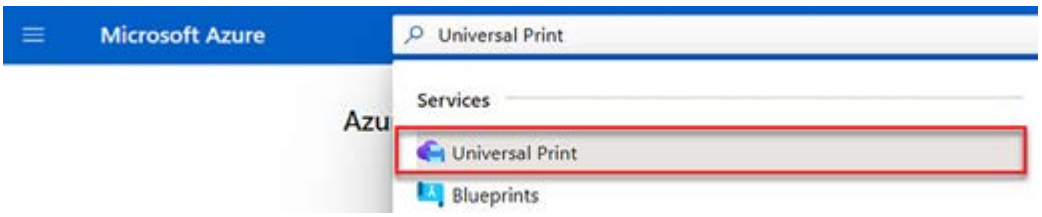


Figure 15.12: Universal Print – Azure portal

3. If you see the following error, make sure you have a Universal Print license assigned to the admin account that is logged in.



Figure 15.13: Universal Print subscription prompt

Before we can configure and manage, we will need to register printers. Let's dive into printer registration.

Register a Universal Print ready printer

The process for registration varies by printer vendor. For exact steps on registering a Universal Print ready printer, refer to the corresponding printer vendor's documentation.

Here is an example flow of registering a Lexmark printer that has integrated Universal Print within its firmware:

1. Go to the printer's configuration page. Typically, you may do this by going to the printer's embedded web server page in a web browser using the IP address of the printer. Select **Network/Ports** under **Settings**.

   Provide a **friendly printer name** and click on the **Register** button.

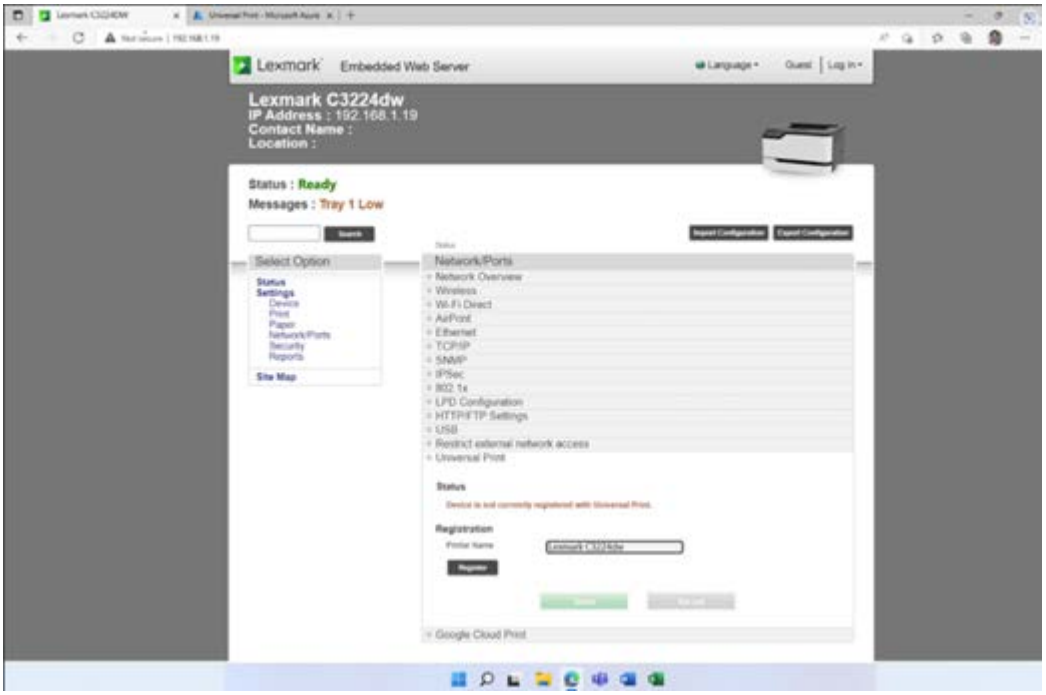


Figure 15.14: Universal Print – Lexmark Network/Ports

2. You will be prompted for the Microsoft Entra ID's device login flow. This will require you to go to `https://microsoft.com/devicelogin` from a managed device on which you can log in using your Universal Print or Global Administrator account. Since we are already on the managed device and doing this in a web browser, you may just click the link. Before clicking the link, **copy** the code that was generated already.

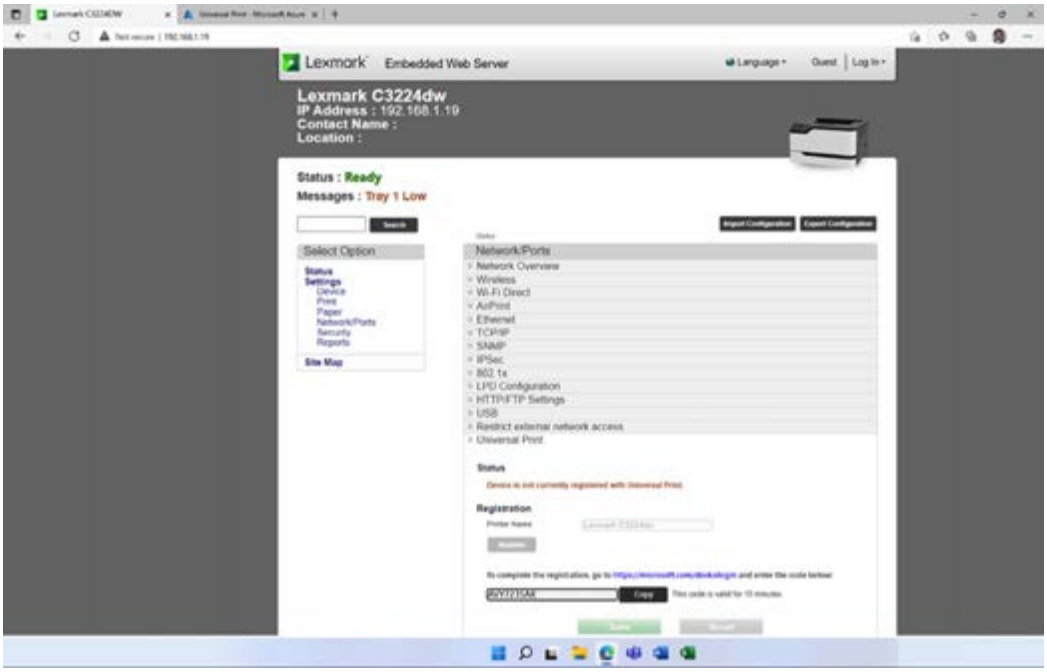


Figure 15.15: Universal Print – Lexmark device code

3. Paste the code and click on the **Next** button.

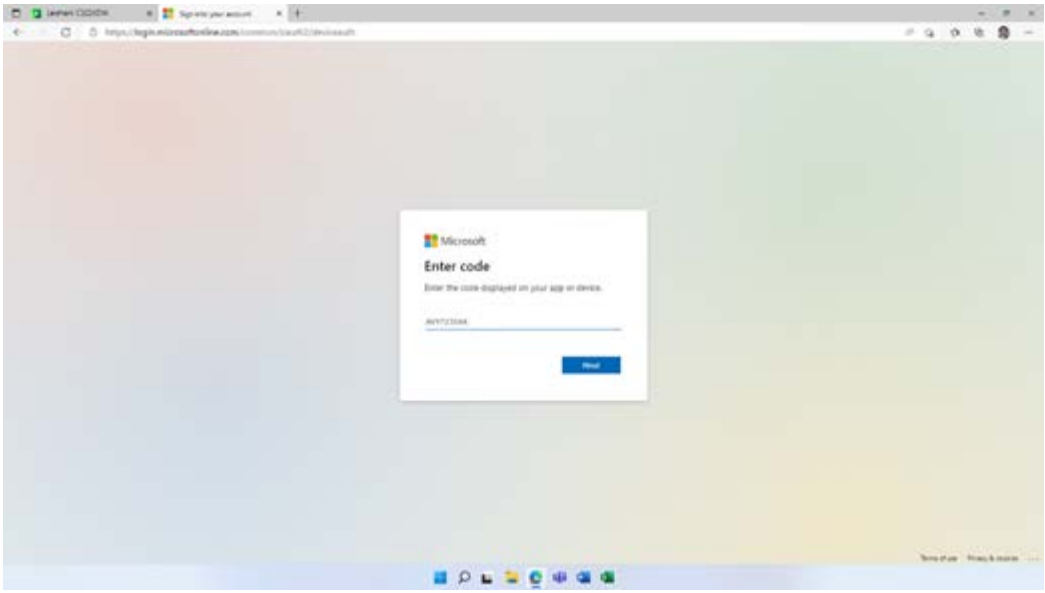


Figure 15.16: Universal Print – log in with device code

4. When prompted, log in with your Print Administrator, Global Administrator, or printer technician account.

   If you are registering a printer from a given vendor for the first time, you may have to approve their application in your Entra ID tenant. This can be automated if you log in with your Global Administrator account on the first printer registration for a given vendor.

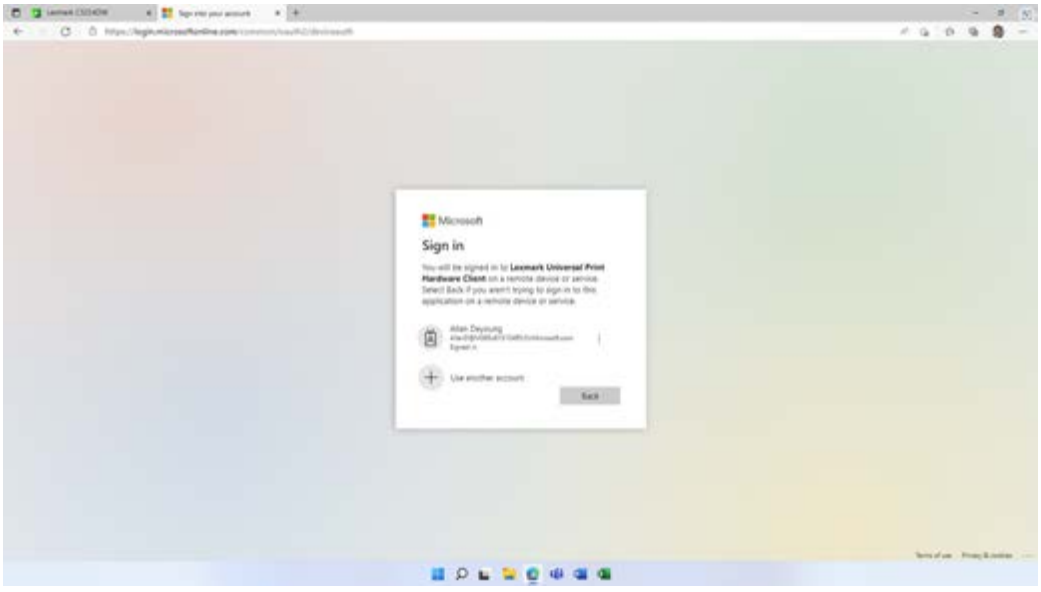


Figure 15.17: Universal Print – Sign in (select account)

5. Review the confirmation that the printer is successfully registered.

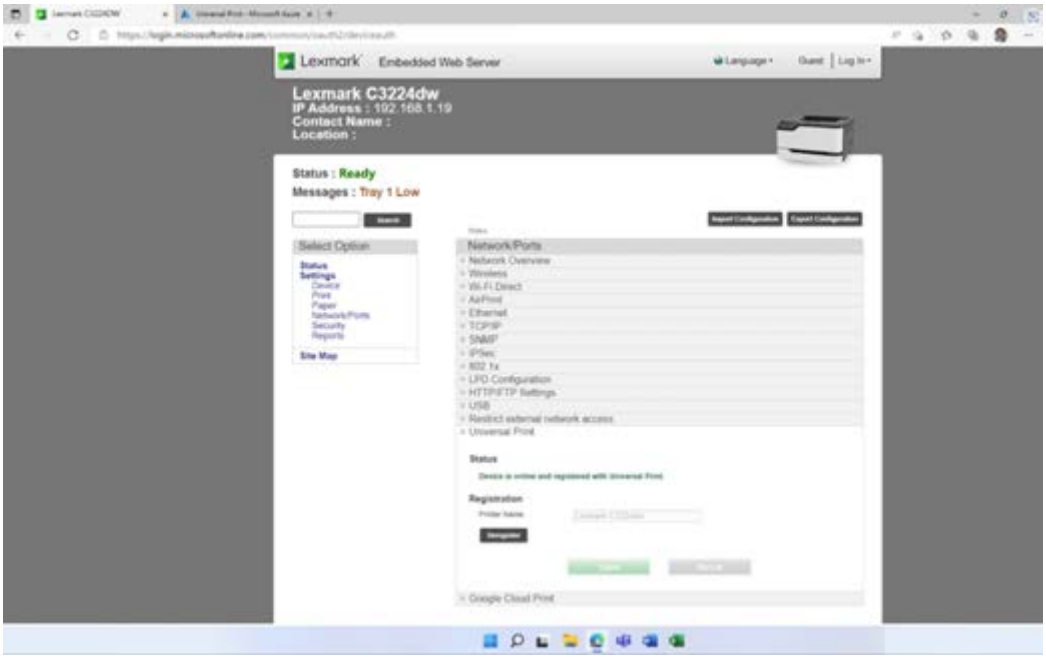


Figure 15.18: Universal Print – registration confirmation

6. Verify that the printer is successfully registered by going to the **Printers** page on the Universal Print admin portal.

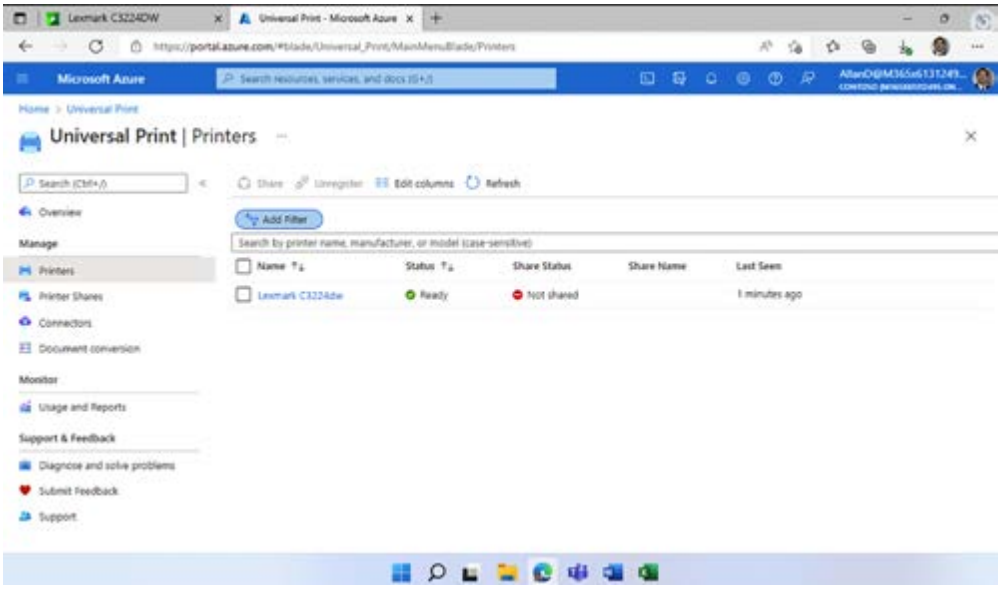


Figure 15.19: Universal Print – Printers in the portal

Register printer(s) with the Universal Print connector

In this section, we're explaining the steps on how to configure the Universal Print connector. Connectors are a great option for older printer models and smoothen the migration to Universal Print, and they save costs by preventing the capital expenditure required to replace a whole printer fleet. You may register more than one printer from the same connector.



You can also install the connector software on one of your existing legacy print servers and register printers with Universal Print. This way, you can support both print deployments in parallel as you transition to the cloud.

Here are the steps to set up a connector:

1. Prepare a host to install the Universal Print connector. The connector host may be on a physical or virtual desktop, that is, on the same network as your printers.
2. Download the latest Universal Print connector here: `https://aka.ms/UPConnector`.
3. To install the Universal Print connector, click **Install**:

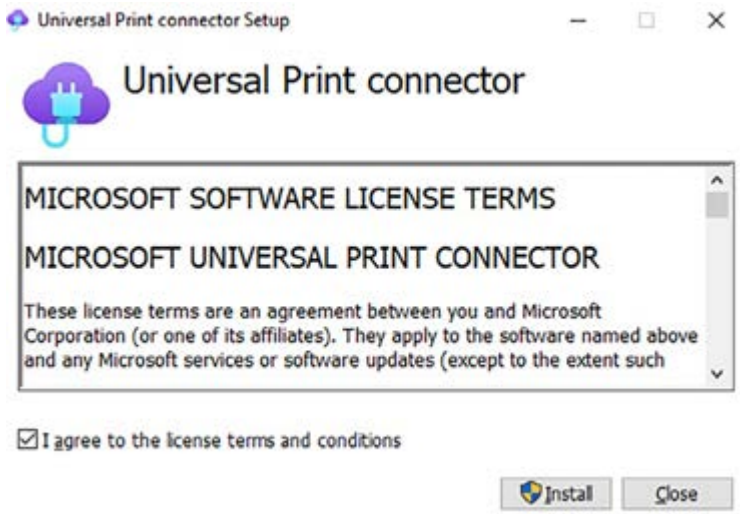


Figure 15.20: Universal Print – connector setup

4. Once the installation is ready, click on **Launch**:



Figure 15.21: Universal Print – connector setup successful

5. Click on **OK** to confirm the diagnostic data prompt.
6. Click on **Login**:

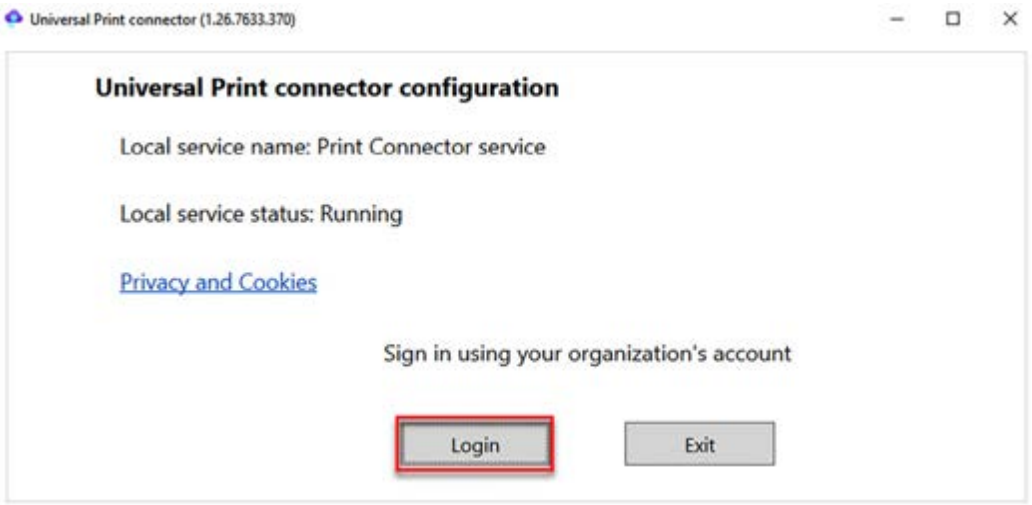


Figure 15.22: Universal Print – connector login

7. Log in with your Print Administrator, Global Administrator, or printer technician account.
8. Enter a name for the connector – the connector will show up later in the Universal Print admin portal – and click on **Register**:

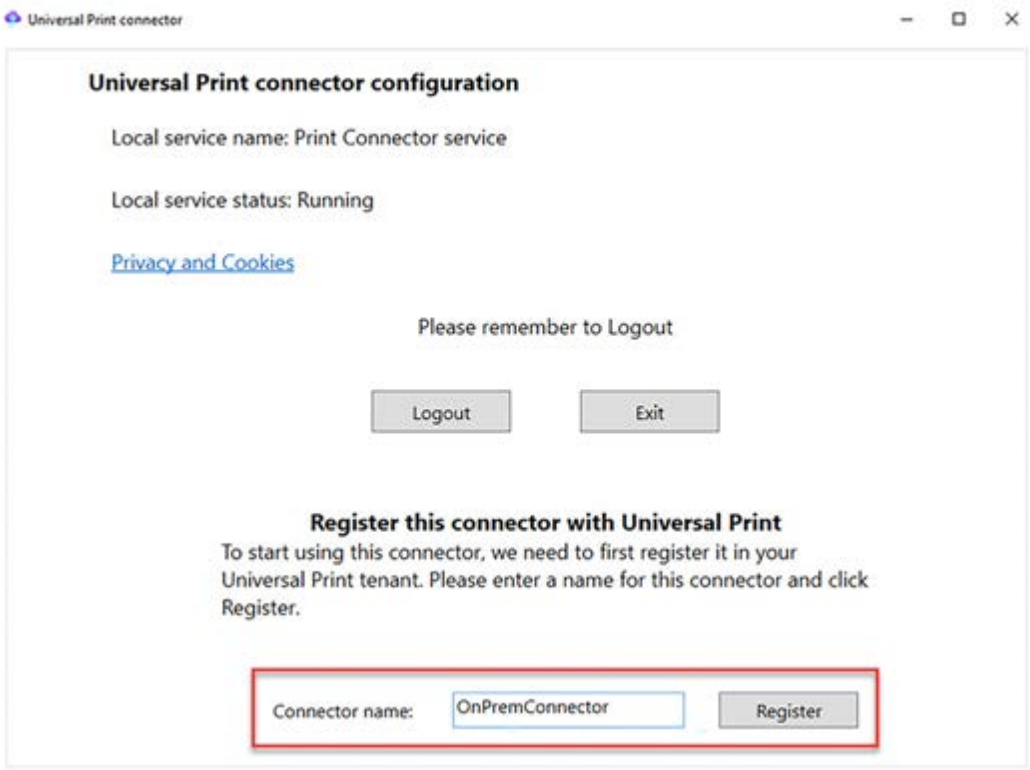


Figure 15.23: Universal Print – connector registration

The connector will now be registered with Universal Print.

9. In the **Connectors** menu, you'll see the connector name show up:

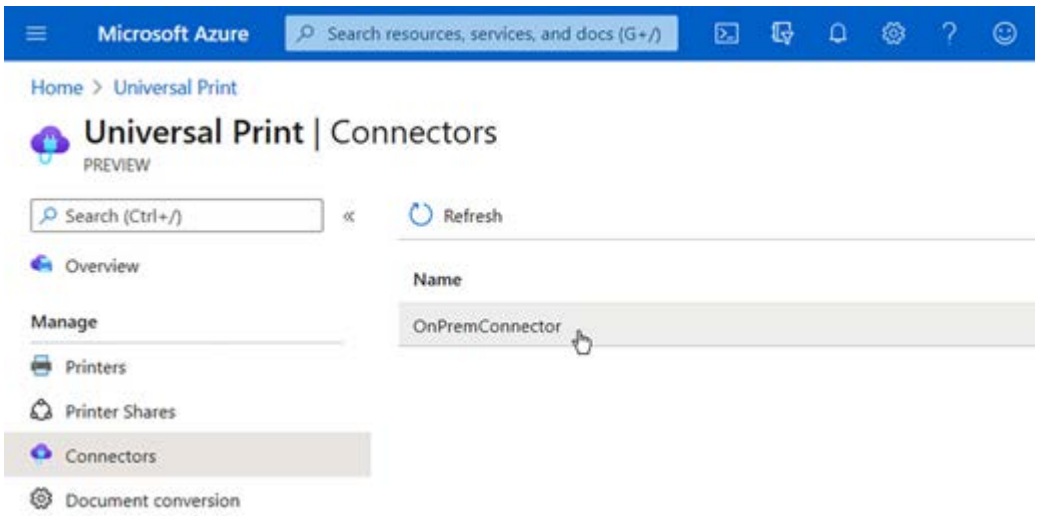


Figure 15.24: Universal Print – connectors page in the portal



The print connector will be created as a device in Microsoft Entra ID – as a device object with an object ID.

You can see an example of how that looks in the Azure portal here:

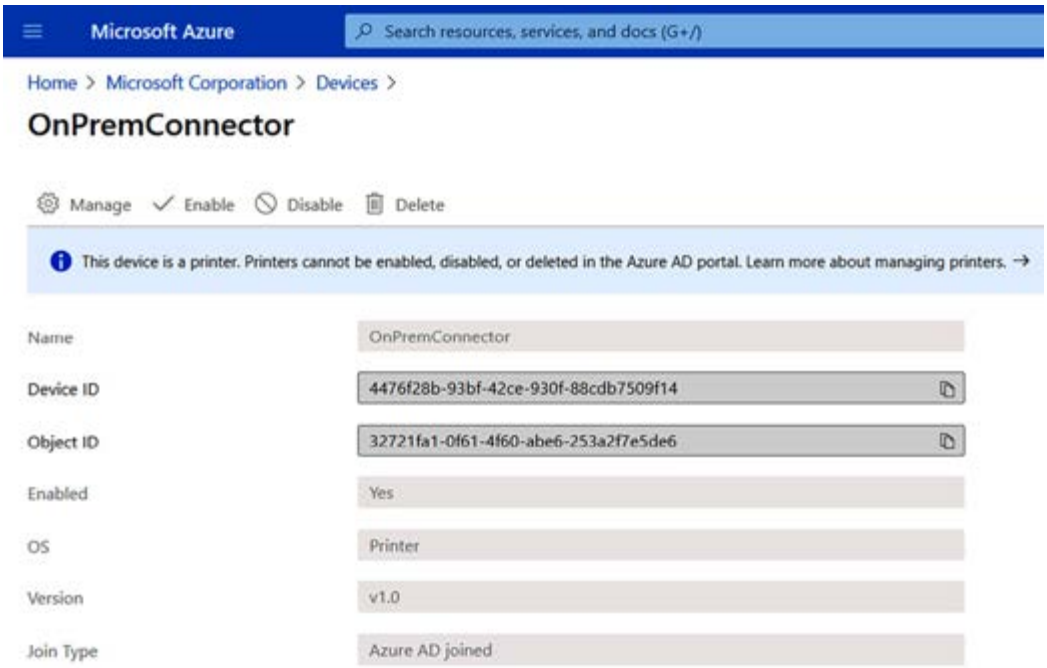


Figure 15.25: Entra ID – connector properties

10. In the Universal Print admin portal, you can click on the connector name to see some of the details of that specific machine and its status:

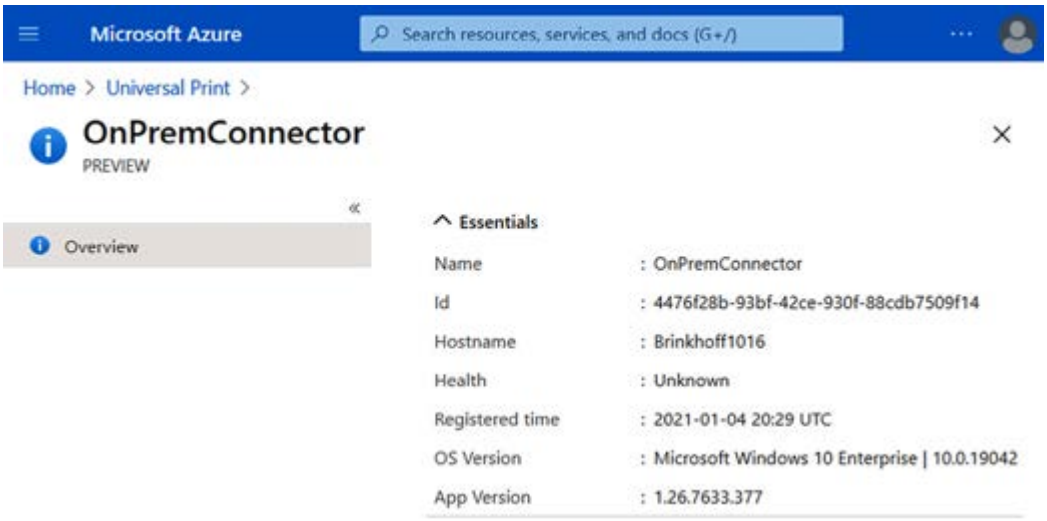


Figure 15.26: Universal Print – Connector details

11. If the printers you are registering via Universal Print have any secure release (other than scanning the QR code with a mobile phone) configured, then you will need to perform an additional step – enable Hybrid Entra ID configuration on the Universal Print connector. This step is *optional* and is required only for secure release.

The following step to enable Hybrid Entra ID configuration can be performed only if the tenant has Hybrid Entra ID enabled. For exact steps to enable Hybrid Entra ID configuration for a tenant, click on the **Learn More** link on Connector.

Enable hybrid Entra ID configuration via the Universal Print connector

1. Activate hybrid Entra ID in the Universal Print connector by ticking the **On** radio button:

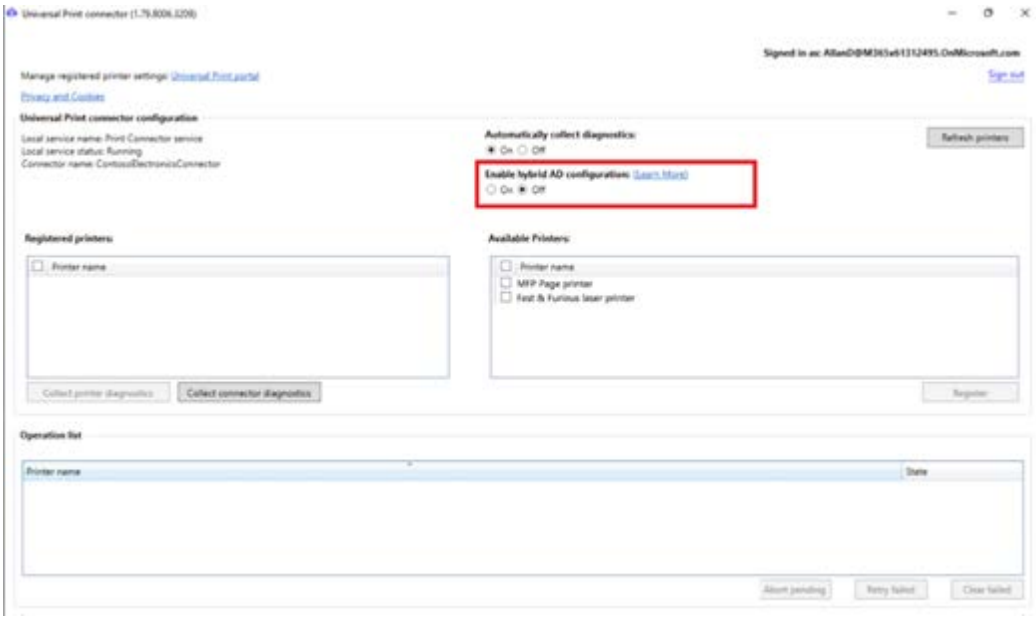


Figure 15.27: Universal Print – connector hybrid Entra ID option

2. Register one or more printers from the connector. Printers that are already installed on the connector host will show up under the **Available Printers** list. Select one or more printers and then click on **Register:**



The list of available printers is detected from the printers attached to the desktop/server you install the printer connector on.

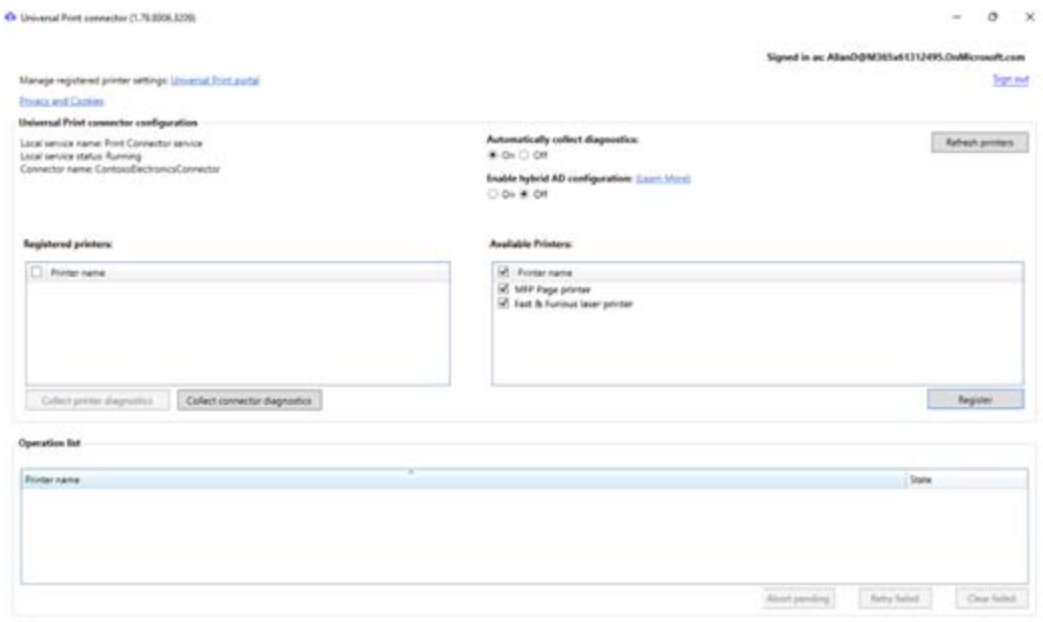


Figure 15.28: Universal Print – connector registering printer(s)

3. The printers are added to the cloud. The state is **In progress**. It may take a few seconds for each printer to be registered.

   Like Universal Print ready printers, you can verify if the printer is successfully registered on the **Printers** page of the Universal Print admin portal under **Printers**.

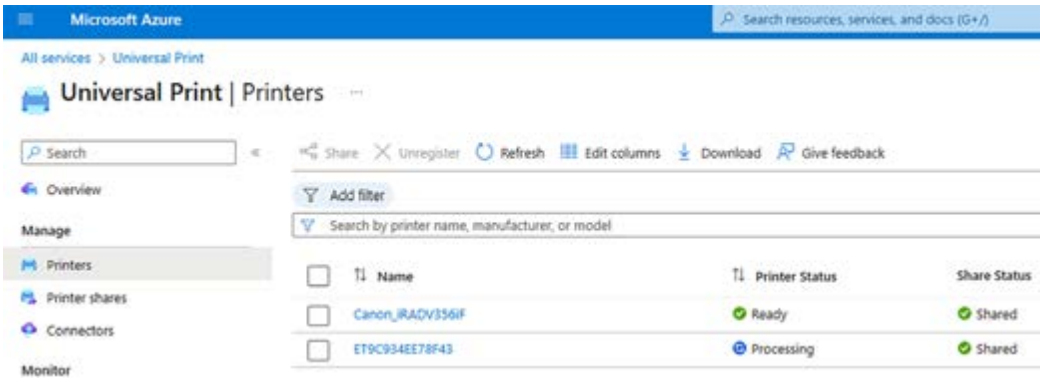


Figure 15.29: Universal Print admin portal

Create a printer share for the printer

End users do not have direct visibility of the printer. Users can print to a printer share only. To create a printer share:

1. Go to the Universal Print admin portal and open the **Printers** page. Printers that are not shared will have a **Share Status** value of **Not shared**.

2. Select the printer(s) you want to share. Click on **Share:**

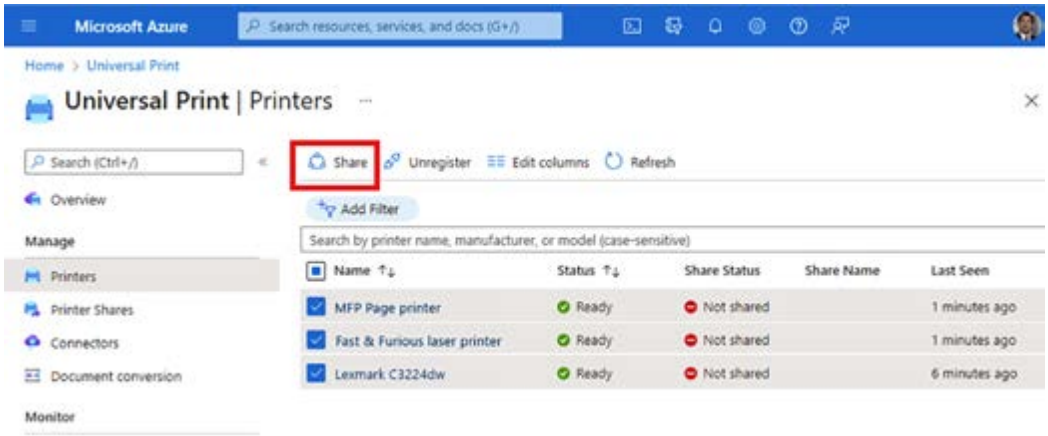


Figure 15.30: Universal Print – create a printer share

3. While sharing, you will be asked to configure who can access the printer share. You may select one or more security groups that contain the users who need to have access to the given printer shares, and then click on the **Share Printer** button:

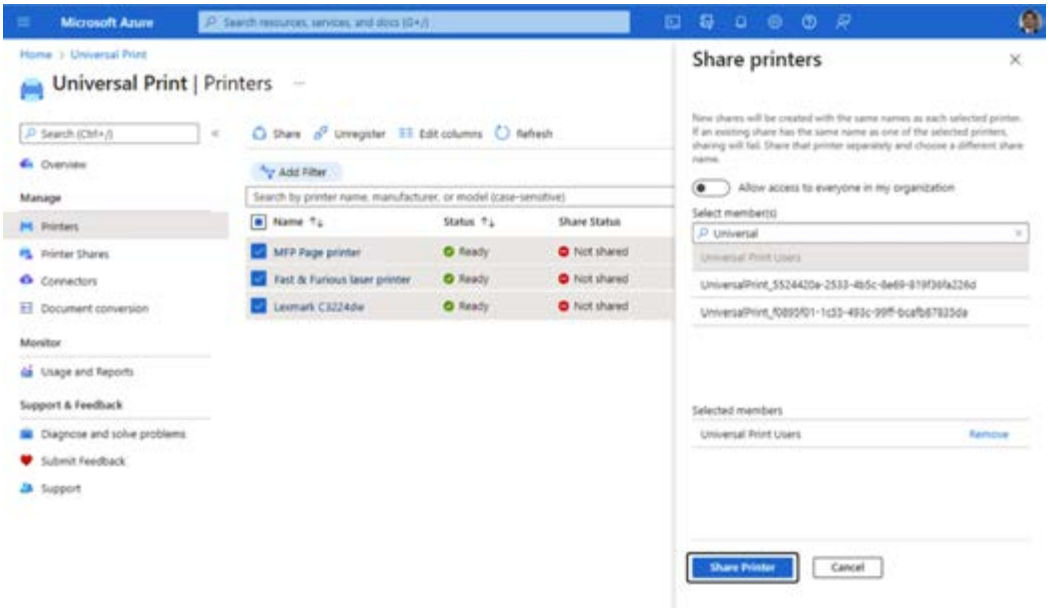


Figure 15.31: Universal Print – printer share access configuration



Did you know you can also select the **Allow access to everyone in my organization** option to allow all users to print to the given printer share(s)?

The printer share access configuration may be updated later as well by going to the **Printer shares** page in the Universal Print portal and clicking on the corresponding printer share.

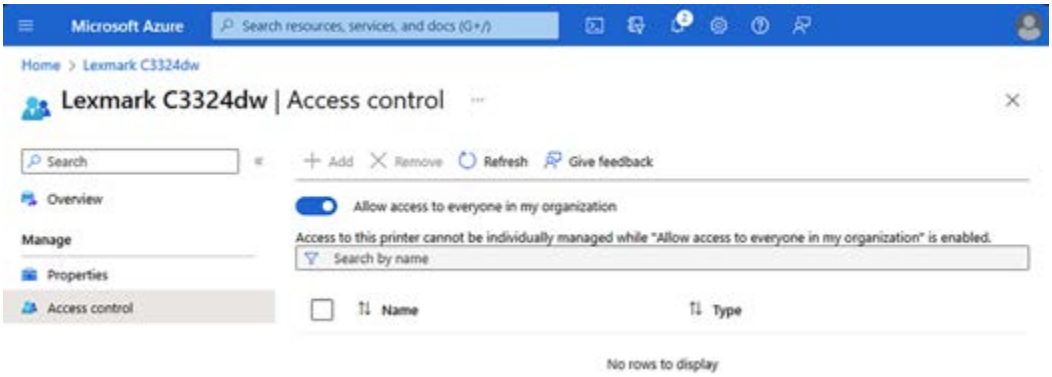


Figure 15.32: Universal Print – printer share access control

4. Once the printers are shared, you can see the **Share Status** values changing **to Printer Shared**.

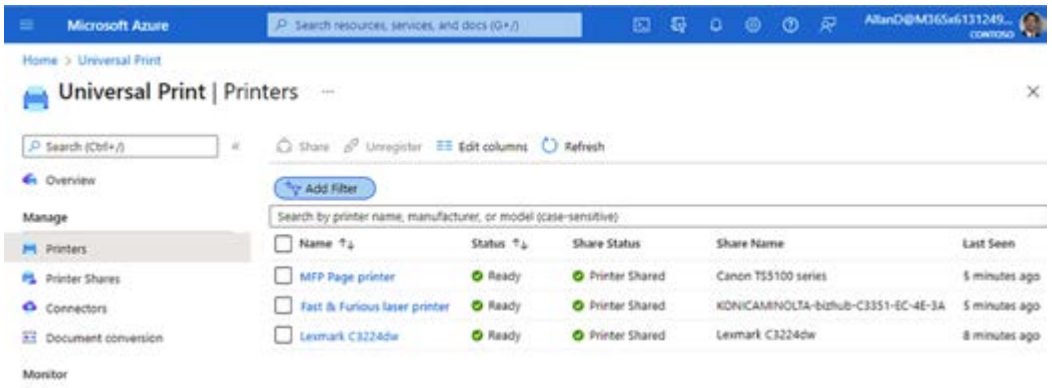


Figure 15.33: Universal Print – printer share success

5. You may optionally configure the secure release for one or more printers. To do so, click on the printer name and then go to its **Properties** page. Now, click on the **Job release options** tab, select the **QR code** option, and click on the **Save** button.

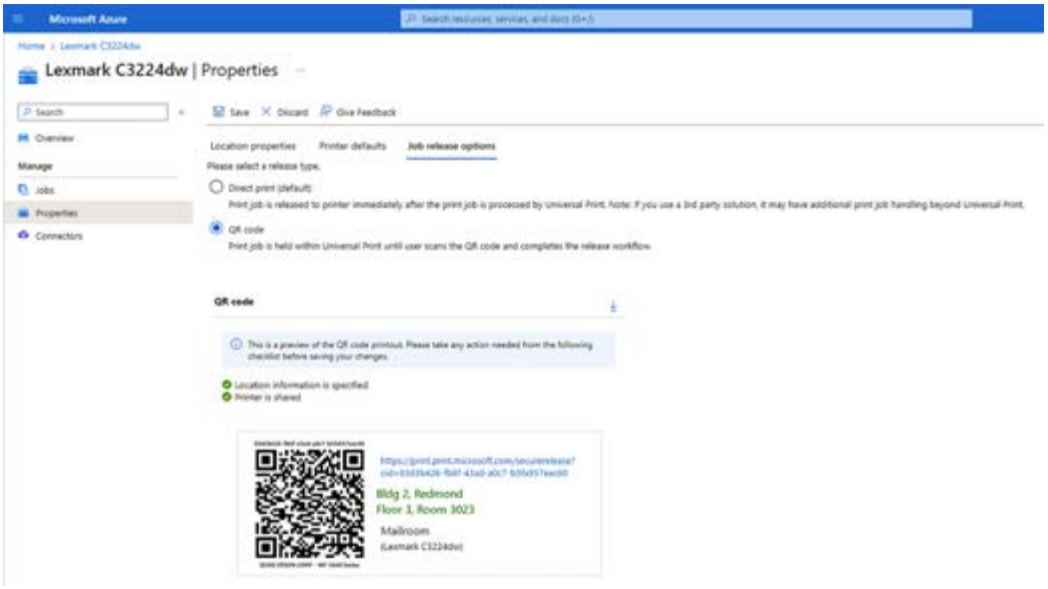


Figure 15.34: Universal Print – secure release (QR code)

6. Click on the download button to get the QR code in a PDF document. You may print the QR code and stick it on the printer. End users can then scan this QR code with their mobile phones and release their print jobs.

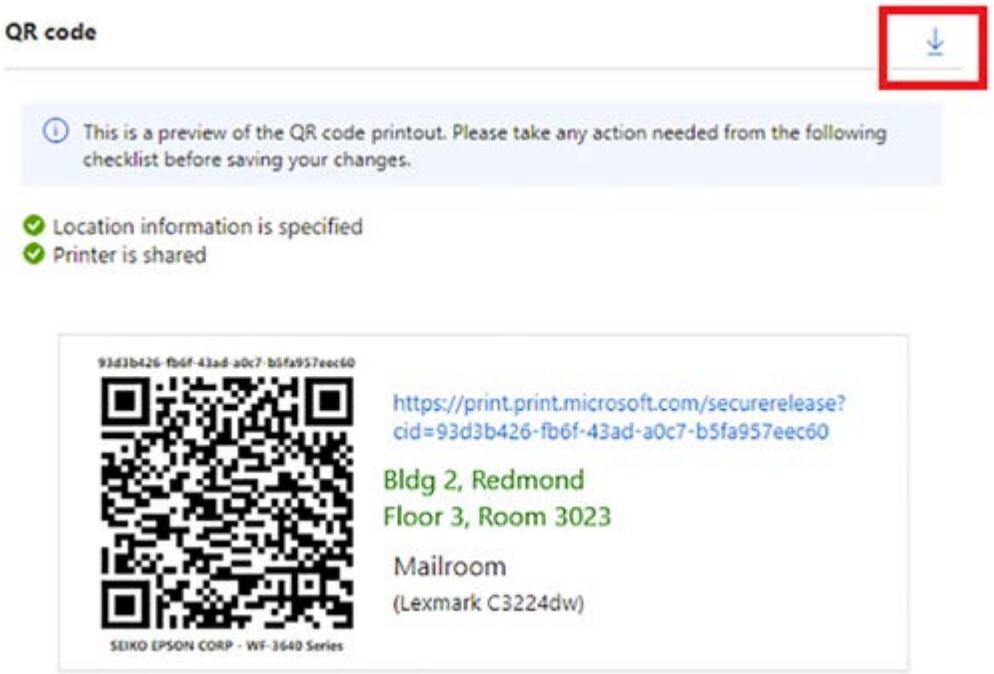


Figure 15.35: Universal Print – download QR code

We are almost ready. Let's move on to the next section, which will explain how to test your printer shares!

Test your Universal Print printer and printer share

In this section, you'll learn how to test your printer shares to confirm that the configuration happened successfully. After succeeding, you will be an official Universal Print expert!

1. First, you need to log on as an Entra ID user to your Windows 365 Cloud or physical PC environment that is assigned to one of the previously shared printers within Universal Print.

2. Search for **Printers & scanners** in the Start menu and click on **Add a printer or scanner:**

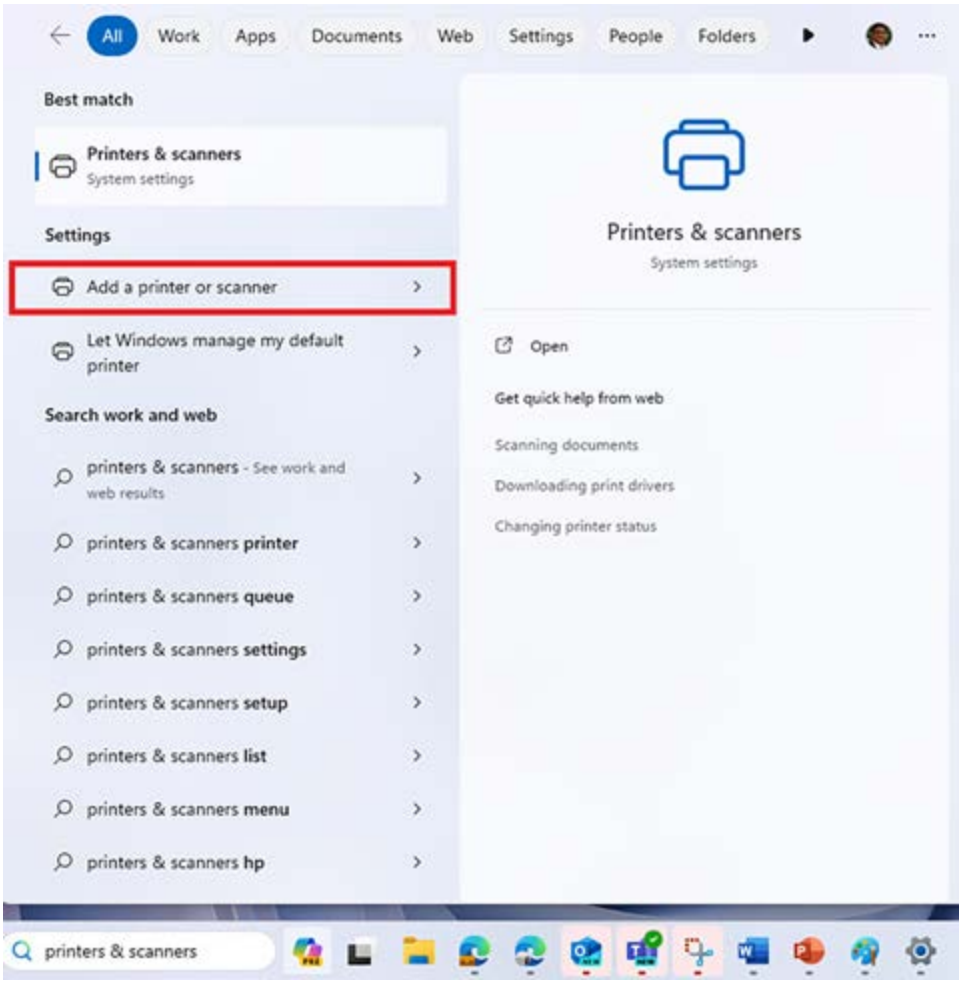


Figure 15.36: Windows search – Windows 11

3. Click on **Add device.**

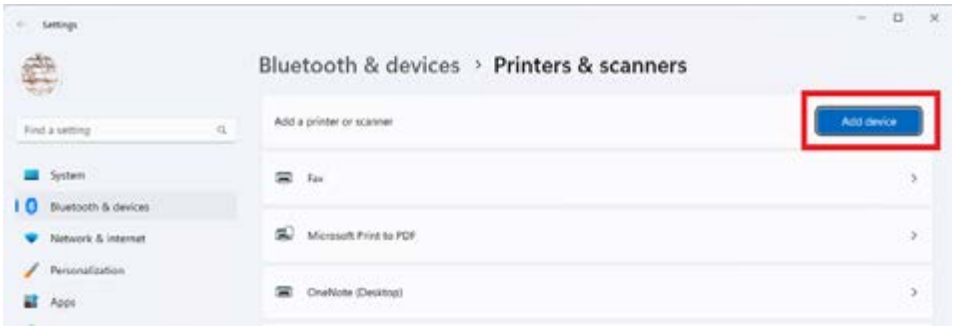


Figure 15.37: Printers & scanners – Windows 11

4. You may then need to click on **Add device** next to the printer you want to add.

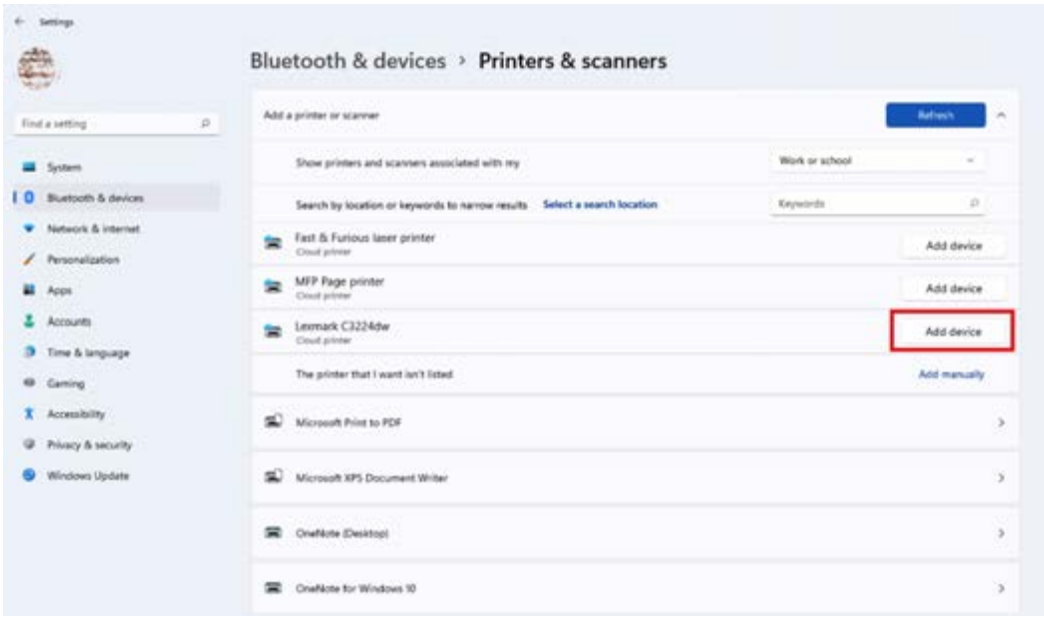


Figure 15.38: Printers & scanners – Add device (printer)

5. The printer has now been added and is ready to be tested. Click on the recently installed printer at the bottom of the list.



Figure 15.39: Printers & scanners – installed printer(s)

6. Click on **Print test page**. The test page will be sent to the printer. You can open the print queue to see if something happens:

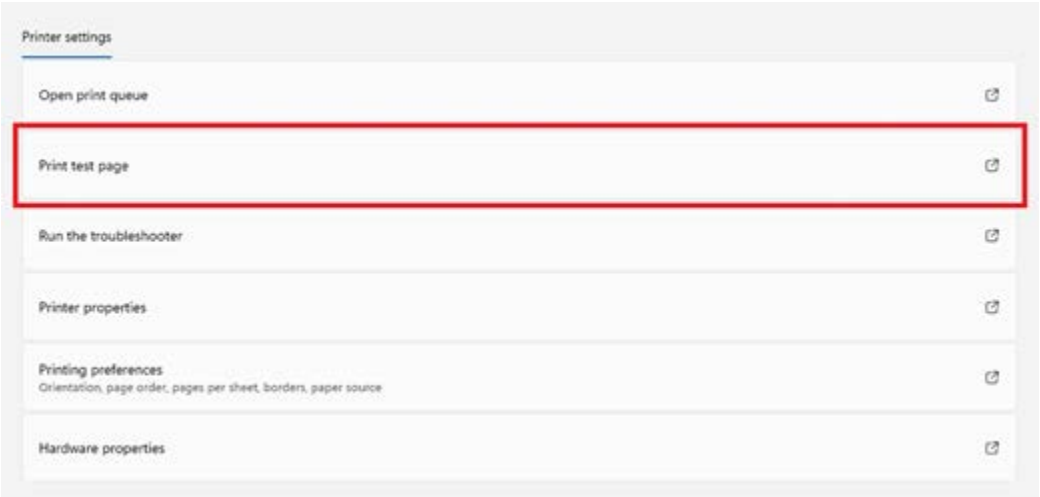


Figure 15.40: Printers & scanners – print a test page

7. If everything goes fine, the print job should be available and listed in the Universal Print admin portal too. You can find the jobs in the Universal Print portal by clicking on the corresponding printer, followed by **Jobs**. You should see the job with the status **Completed** if there is no secure release on the printer. If there is secure release configured for the printer, then the print job will be in a **Paused** state until the user releases the job. Great job!

In the next section, you'll learn how to publish printers via Microsoft Intune.

Assigning and deploying cloud printers with Microsoft Intune

In the previous section, you learned about all the basics – as well as the manual process – of assigning printers. This process is also possible to perform via Intune (as explained earlier) as a more enterprise-ready approach to, for example, assigning multiple printers across the globe to many of your users.

You can now easily assign Universal Print printers using Microsoft Intune via the new settings catalog integration that you can find under **Printer Provisioning**.

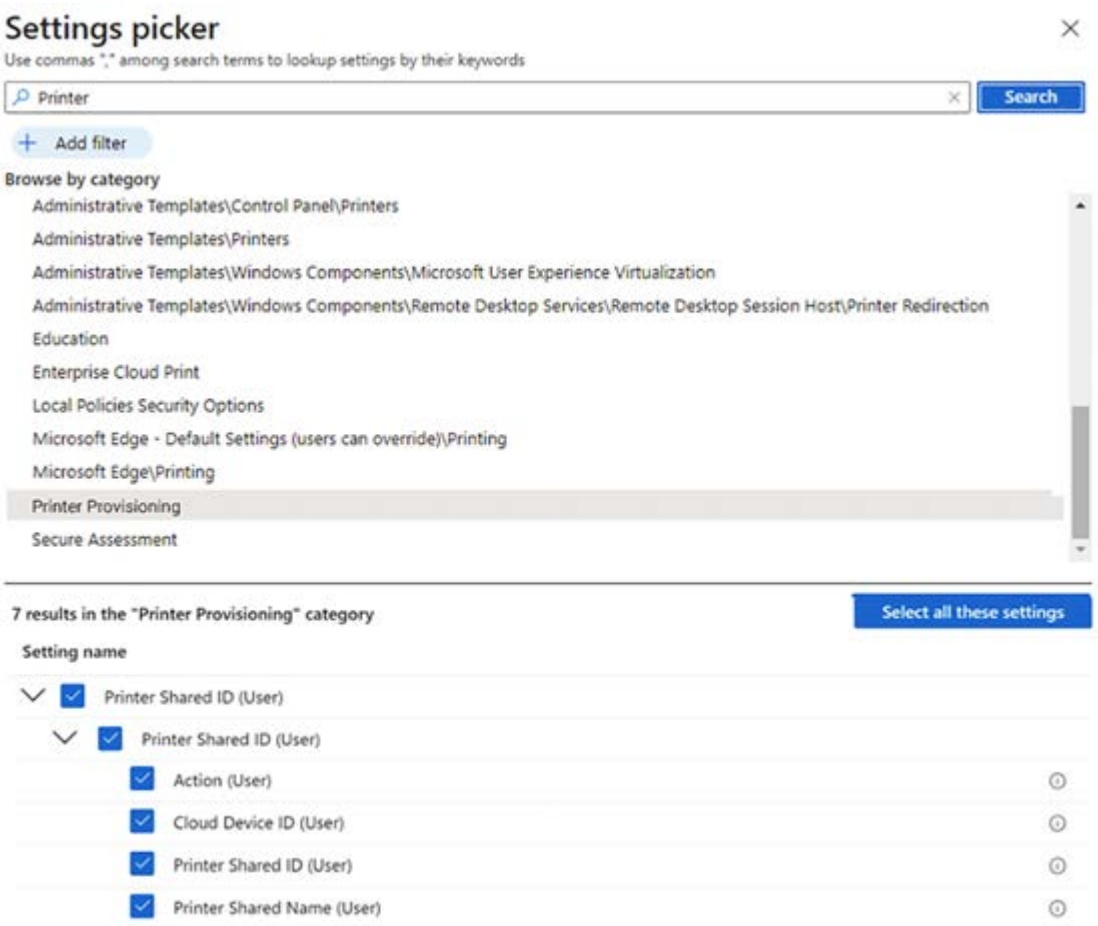


Figure 15.41: Microsoft Intune – Settings picker

Once you select **Printer Shared ID (User)**, you need to fill in the Universal Print **Printer Shared Name** (User) and Printer Shared ID (User).

You can find the ID inside the Microsoft Azure Universal Print admin portal under your printer's **Devices** menu (see the following example).

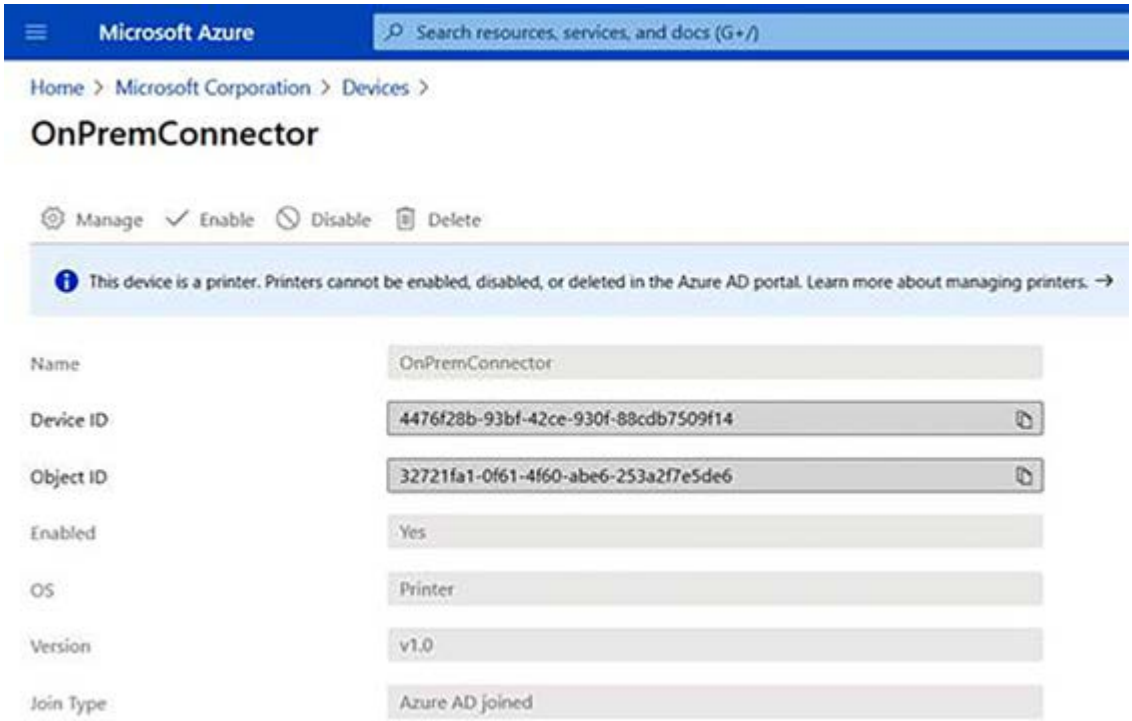


Figure 15.42: Universal Print printer's Devices menu

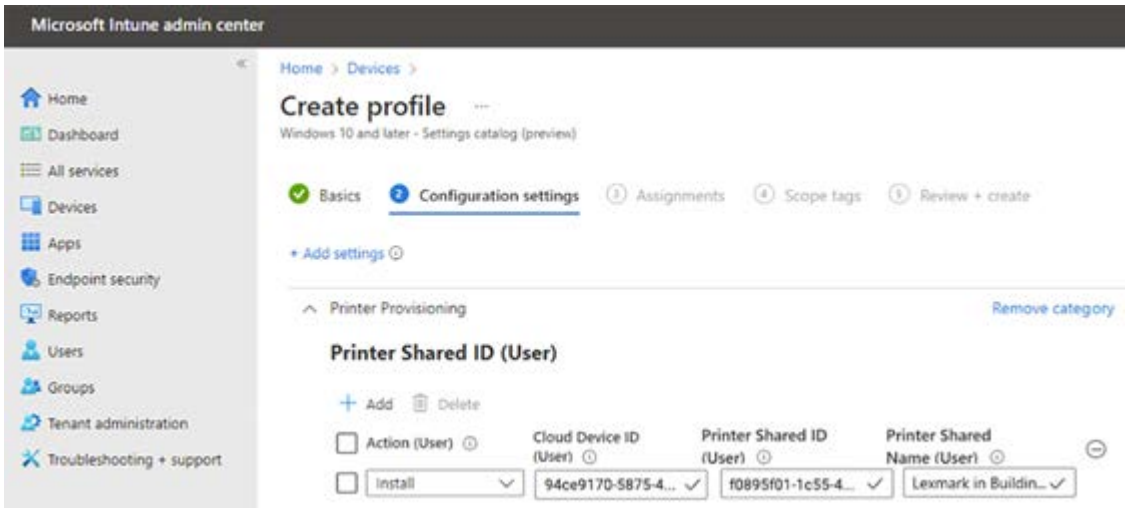


Figure 15.43: Microsoft Intune – Create profile

Once you are ready, you can track the printer assignments using the policy deployment monitoring dashboard, under the policy name.

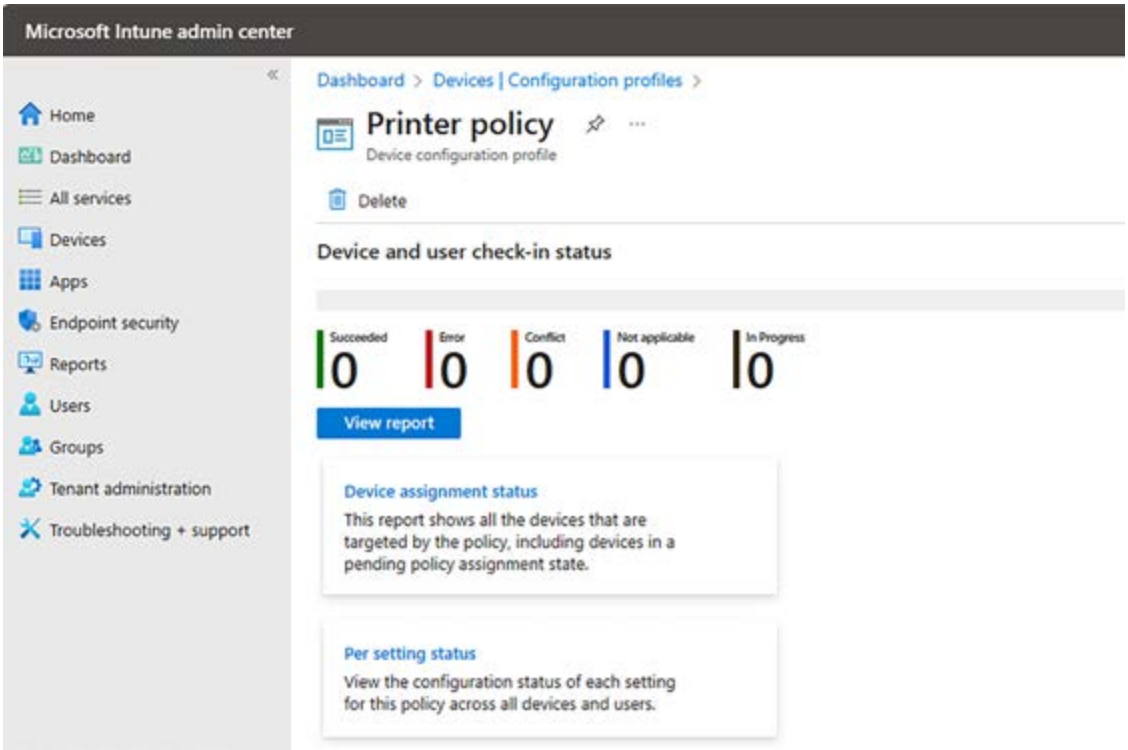


Figure 15.44: Microsoft Intune – check status

Summary

In this chapter, you've learned about a new Microsoft 365 service called Universal Print, how to configure the service, and how to publish printers to your endpoints via Intune.

In the next chapter, we're going to talk about other devices that you can manage with Intune.

Questions

1. What port needs to be open in the firewall in order to use Universal Print?
    a. `TCP - 443`
    b. `TCP - 445`
2. Are print jobs with Universal Print sent to the cloud encrypted?
    a. Yes
    b. No

3. Does Universal Print support zero-trust?
    a. Yes, all traffic goes over the internet over SSL
    b. No

Answers

1. (a)
2. (a)
3. (a)

Further reading

If you want to learn more about Universal Print after reading this chapter, please use the following free online resources:

- Universal Print – Intune provisioning via `https://aka.ms/UPintunetool`
- Universal Print – Get started via `https://aka.ms/UPdocs`
- Universal Print – Secure release via `https://aka.ms/UPqrcoderelease`
- Universal Print – Simulated experience via `https://aka.ms/GetToKnowUniversalPrint`

Get This Book's PDF Version and Exclusive Extras

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

Note: *Keep your invoice handy. Purchases made directly from Packt don't require one.*

UNLOCK NOW



Section IV

Troubleshooting and Community

In this section, you will learn from the writers about the most common deployment- and networking-related errors they see in the field and how to counter and resolve them.

This part of the book comprises the following chapters:

- *Chapter 16, Troubleshooting Microsoft Intune*
- *Chapter 17, Troubleshooting Windows 365*
- *Chapter 18, Community Help*

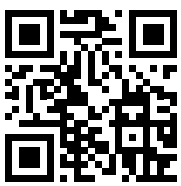
16

Troubleshooting Microsoft Intune

This chapter offers you a comprehensive guide to resolving common deployment issues encountered with Windows 10 Enterprise. Drawing upon the authors' extensive two-decade experience in deploying various Windows configurations, this online bonus chapter is packed with practical tips, effective fixes, and insider tricks to ensure seamless deployment processes.

To access this bonus content, scan the provided QR code or visit the specified link:

`https://packt.link/7YCAW`



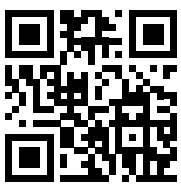
17

Troubleshooting Windows 365

This chapter equips you with the essential skills to pre-emptively tackle errors in deploying Windows 365 Cloud PC. Covering a spectrum of troubleshooting techniques, this online bonus chapter prepares you to respond proactively to potential errors, ensuring successful cloud PC deployments in your environment.

To access this chapter, scan the QR code included below:

`https://packt.link/h4vTm`



Get This Book's PDF Version and Exclusive Extras

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.

***Note**: Keep your invoice handy. Purchases made directly from Packt don't require one.*

UNLOCK NOW



18

Community Help

Community hall of fame

You can find all kinds of people who contribute to the Microsoft Intune, Windows 365, and Azure Virtual Desktop enterprise mobility communities. Some are Microsoft MVPs, while others are working/have worked for Microsoft – and all are great community ambassadors!

We have gathered all the sources of help you could use in this chapter. In this way, you'll have everything in one place, just in case.

CAUTION!

If you go through the following list, your mind will be blown by all the top-notch Intune and Windows 365 experts. Go look them up on LinkedIn and X!

Jannik Reinhard

Florian Salzmann

Mahammad Kubaib

Aavisek Choudhury

Andy Jones

Joost Gelijsteen

Somesh Pathak

Shehan Perera

Oktay Sari

Johan Vanneuville

Andrew Taylor

Bernhard Tritsch

Gil Kirkpatrick

Panu Saukko

Johan Arwidmark

Kim Oppalfens

Greg Ramsey

Suguru Kunii

Garth Jones

Sylvain Cortes

Andre Oliveira

Jon Jarvis

Davina Armstrong-Cruz

Aresh Sarkari

Jakub Piesik

Dominiek Verham

Doug Petrole

Ritsuko Nishibata

Trond Eirik Haavarstein

Thomas Marcussen

Morten Pedholt Pedersen

Ruben Spruijt

Stefan Schörling

Ronni Pedersen

James Kindon

Matthew Hudson

John Marcum

Kristin Griffin

Raphael Perez

Kent Agerlund

Jean-Sébastien Duchêne

Niall Brady

Miklos Cari Sivila

Jörgen Nilsson

Jon Towles

Freek Berson

Peter Daalmans

Dubravko Marak

Roger Zander

Hasitha Willarachchi

Rory Monaghan

Danny van Dam

Prajwal Desai

Octavio Rdz de Santiago

Rafael Silva

Bram Wolfs

Kenneth van Surksum

Tim De Keukelaere

Benoit Lecours

Nicolas Bonnet

Thiago de Oliveira

Peter van der Woude

Mirko Colemberg

Gerry Hampson

Anoop Nair

Thomas Poppelgaard

Robert Milford

Nickolaj Andersen

Jan Ketil Skanke

Mike Terrill

Maurice Daly

Nick Hogarth

Paul Winstanley

Eswar Koneti

Marius Skovli

Sandy Yinghua Zeng

Mark Plettenberg

Tom Degreef

Oliver Kieselbach

Simon Binder

Martin Bengtsson

Micha Wets

Matthew Levy

Bas van Kaam

Doug Wilson

Adam Gross

Bryan Dam

Thomas Kurth

Timmy Andersson

Yutaro Tamai

Jordan Benzing

Tim Hermie

Peter Klapwijk

Ben Reader

Neil McLoughlin

Kenta Osuka

Fredrik Brattstig

Patrick Koehler

Stefan Dingemanse

Michael Mardahl

Joymalya BasuRoy

Katy Nicholson

Rudy Ooms

Mattias Melkersen

Davide Salsi

Torbjörn Granheden

Dujon Walsham

Nathan Blasac

Jacob Shackelford

Shabaz Darr

Ben Whitmore

Sander Rozemuller

Benoit Hamet

Jeremy Moskowitz

Manish Bangia

Mahmoud A. Atallah

Nicklas Ahlberg

Dean Ellerby

Tobias Almén

Jóhannes Kristjánsson

Rahul Jindal

Harvansh Singh

Niels Kok

Ryan Mangan

Community events to participate in!

The following community events around modern management and Windows 365 are worth looking out for in 2024 and onward!

MMS — Minnesota and Fort Lauderdale

The *Midwest Management Summit* is a 4-day conference purposely capped to just 750 attendees so that nobody gets lost in the crowd.

Speakers have time to meet and talk to you. There's no rushing people out of a session to get the next speaker going, and there's time to absorb what you see and talk it over with speakers and other attendees. Check out the website for more information: `https://mmsmoa.com/`.



Figure 18.1: Midwest Management Summit

MEM Summit — Paris

The *Modern Endpoint Management Summit* 2024 EMEA Edition consists of an event dedicated to exploring the latest trends, innovations, and best practices in the field of endpoint management. This has been arranged after a successful in-person event in 2023 at a campus in Paris.



Figure 18.2: Modern Endpoint Management Summit

Workplace Ninja Summit – Europe

Workplace Ninja Summit is another amazing community event to learn about all things Intune and Windows 365. Their goal is to share knowledge with the community and to make workplace management with Microsoft technologies simpler for everybody. Check out the website for more information: `https://www.wpninjas.eu/`.



Figure 18.3: Workplace Ninja Summit

Windows 365 Community

Engaging with other people on platforms can be valuable as you can learn from their experiences, ask questions, get inspired, and more.

We are therefore excited to share that we have launched a brand-new Discord server. We as a community would like to engage with you in a way we haven't done before, and more importantly, we want to create a platform where you are able to get your questions answered or discuss topics with other people about Windows 365.

Join now via `https://discord.gg/2UhfvD7qtn` or follow the latest news via `https://W365Community.com`.



Figure 18.4: Windows 365 Community

Windows in the Cloud – video webcast

Dive into the latest Windows 365 capabilities with insights and demos from Microsoft engineers bringing you Windows in the Cloud! Learn how to easily deploy and manage cloud PCs and create a protected and productive experience for your end users! Join host Christiaan Brinkhoff as he also brings in members of the Windows 365 community to share best practices and adoption tips. Learn more about it via `aka.ms/WindowsInTheCloud` or `WindowsInTheCloud.com`.

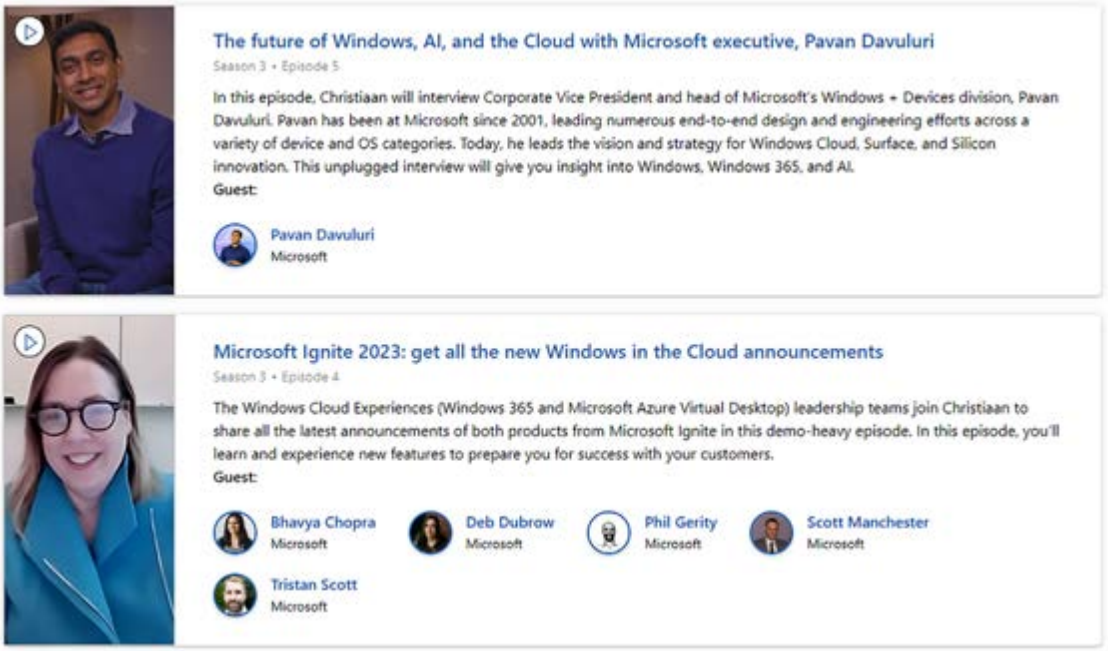


Figure 18.5: Windows in the Cloud - Video webcast

Summary

This was the final chapter of the book, where we saw all the mind-blowing social media channels where you can find some great contributors to the tech community. We hope all the knowledge contained in this book was useful to you and we thank you for completing this journey with us.

Learn more on Discord

To join the Discord community for this book – where you can share feedback, ask questions to the author, and learn about new releases – follow the QR code below:

`https://packt.link/SecNet`

19

Unlock Your Exclusive Benefits

Your copy of this book includes the following exclusive benefits:

- Next-gen Packt Reader
- DRM-free PDF/ePub downloads

Follow the guide below to unlock them. The process takes only a few minutes and needs to be completed once.

Unlock this Book's Free Benefits in 3 Easy Steps

Step 1

Keep your purchase invoice ready for *Step 3*. If you have a physical copy, scan it using your phone and save it as a PDF, JPG, or PNG.

For more help on finding your invoice, visit `https://www.packtpub.com/unlock-benefits/help`.



Note: If you bought this book directly from Packt, no invoice is required. After *Step 2*, you can access your exclusive content right away.

Step 2

Scan the QR code or go to `packtpub.com/unlock`.

On the page that opens (similar to *Figure 19.1* on desktop), search for this book by name and select the correct edition.

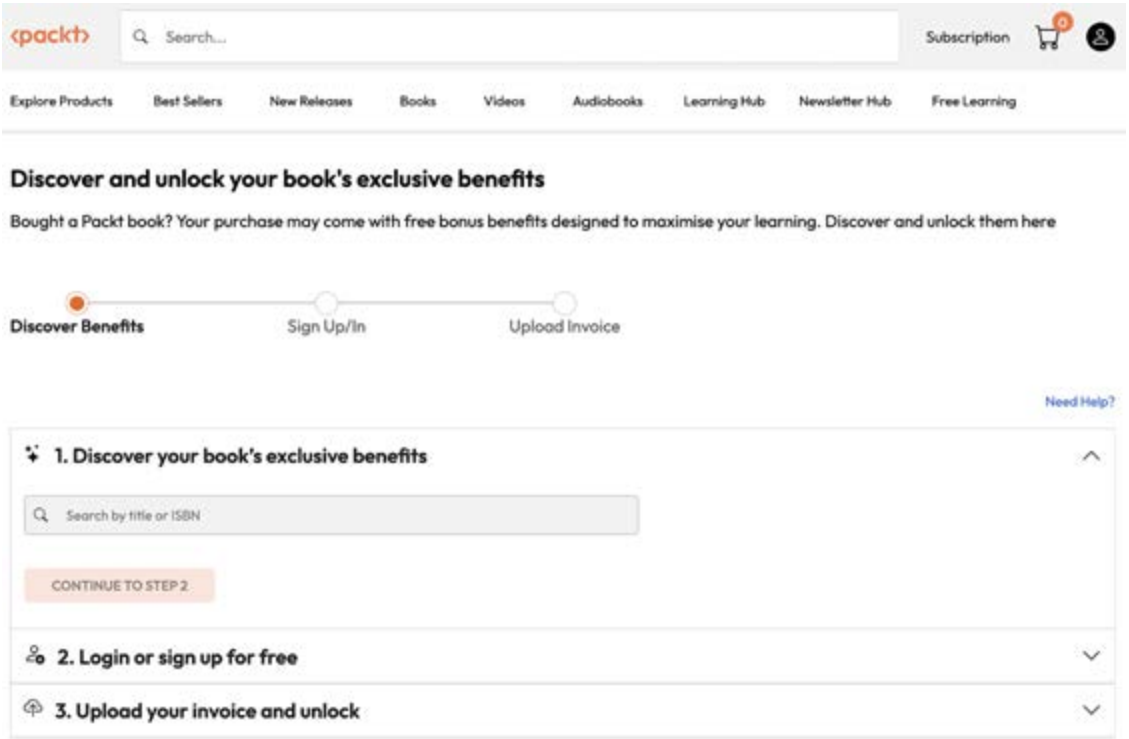


Figure 19.1: Packt unlock landing page on desktop

Step 3

After selecting your book, sign in to your Packt account or create one for free. Then upload your invoice (PDF, PNG, or JPG, up to 10 MB). Follow the on-screen instructions to finish the process.

Need help?

If you get stuck and need help, visit `https://www.packtpub.com/unlock-benefits/help` for a detailed FAQ on how to find your invoices and more. This QR code will take you to the help page.





Note: If you are still facing issues, reach out to `customercare@packt.com`.



packtpub.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

At www.packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Other Books You May Enjoy

If you enjoyed this book, you may be interested in these other books by Packt:

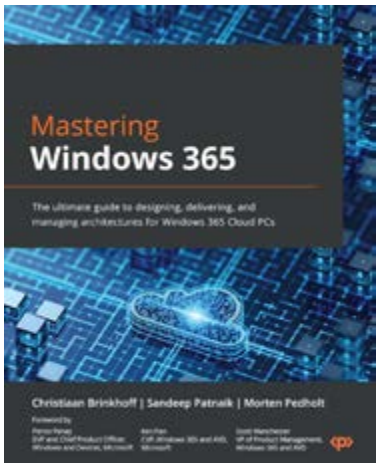


Mastering Windows Server 2022 – Fourth Edition

Jordan Krause

ISBN: 978-1-83763-450-7

- Build a Windows Server from the ground up and implement your own PKI
- Manage your servers with Server Manager, PowerShell, and Windows Admin Center
- Secure your network and data with modern technologies in Windows Server 2022
- Understand containers and where Nano Server fits into the equation
- Discover new ways to integrate your datacenter with Microsoft Azure
- Virtualize your datacenter with Hyper-V
- Round out your understanding of Active Directory, DNS, DHCP, and Group Policy
- Deploy Remote Desktop Services in your environment



Mastering Windows 365

Morten Pedholt

Christiaan Brinkhoff

Sandeep Patnaik

ISBN: 978-1-83763-796-6

- Understand the features and uses of Windows 365 and Cloud PCs
- Extend your existing skillset with Windows 365 and Intune
- Secure your Windows 365 Cloud PC connection efficiently
- Optimize the Cloud PC user experience through effective analysis and monitoring
- Explore how partners extend the value of Windows 365
- Use the available tools and data within Windows 365
- Troubleshoot Windows 365 with effective tips and tricks

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Share your thoughts

Now you've finished *Mastering Microsoft Intune, Second Edition*, we'd love to hear your thoughts! If you purchased the book from Amazon, please `click here to go straight to the Amazon review page` for this book and share your feedback or leave a review on the site that you purchased it from.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Stay Sharp in Cloud and DevOps – Join 44,000+ Subscribers of CloudPro

CloudPro is a weekly newsletter for cloud professionals who want to stay current on the fast-evolving world of cloud computing, DevOps, and infrastructure engineering.

Every issue delivers focused, high-signal content on topics like:

- AWS, GCP & multi-cloud architecture
- Containers, Kubernetes & orchestration
- Infrastructure as Code (IaC) with Terraform, Pulumi, etc.
- Platform engineering & automation workflows
- Observability, performance tuning, and reliability best practices

Whether you're a cloud engineer, SRE, DevOps practitioner, or platform lead, CloudPro helps you stay on top of what matters, without the noise.

Scan the QR code to join for free and get weekly insights straight to your inbox:



`https://packt.link/cloudpro`

Index

A

account protection policies 39

Active Directory (AD) 190, 594

Active Directory-based group policies
migrating from 401-408

Active Directory Domain Services (AD DS) 6, 593

Active Directory Federation Services (ADFS) 252

Administrative Template Language (ADML) 438

administrative templates
configuring 444, 445
OneDrive Known Folder Move configuration 446-449

ADMX files 431
importing 438-444
working 431

Adoption Score 16

Advanced Endpoint Analytics 478, 563-567, 710
accessing, in Intune 564
battery health 570-572
capabilities 563
features 711

Antivirus 415

Antivirus Policies 38

Application Control for Business 38, 644-659

application delivery
via Microsoft Intune 319

Application Programming Interfaces (APIs) 678

application reliability 695, 696

applications
installing, via Enterprise App Management 509-517

applications that bypassing WDAC and how to block them
reference link 508

application types
for deploying 320, 321

apps available in Enterprise App Catalog
reference link 509

Artificial Intelligence (AI) 8
future, in Windows and Intune 575, 576

Assessment and Deployment Kit (ADK) 257

Attack Surface Reduction (ASR) 38, 419

Authenticator Attestation GUID (AAGUID) 623

automatic BitLocker encryption
troubleshooting, on VM 290

Autopilot
automatic BitLocker encryption, configuring 281-289
Company Portal 279, 280
reporting and diagnostics 276-278

Autopilot Profile Standard user 502, 503

Azure Active Directory (Azure AD) 5, 9, 374, 595

Azure Front Door (AFD) 726

Azure Monitor integration 705

Azure Network Connection (ANC) 111

Azure Scale Unit (ASU) 86

Azure Site Recovery (ASR) 486

Azure Virtual Desktop (AVD) 7, 98, 372, 718
service responsibilities 9
versus Windows 365 8

B

Baselines
Azure Monitor integration 705
customizing 700
remediation script 701-704
Windows 365 Frontline 704
battery health 570-572
Bing Chat 13
BIOS update policies, types
supported by HP Connect 35
BitLocker
recovery keys 633-636
BitLocker disk encryption 632, 633
BitLocker drive encryption 38
Bring Your Own Device (BYOD) 6, 21, 26, 49, 50, 70, 176, 315
bulk device actions 179, 180
bulk user actions
via Intune 160
business continuity and disaster recovery (BCDR) 107

C

Center for Internet Security (CIS) 412
certificate revocations 535
confirmation 537
Intune profile trusted certificate, configuring for deployment 538, 539
Intune SCEP certificate profile, creating 541-545
Issuing CA 536
practical scenarios 536, 537
reasons for 535
trust and authentication, ensuring 535
Certificate Signing Request (CSR) 529
ChatGPT plugins 13
Cloud apps 608-610
conditions, types 610-612
cloud attached devices 684
Cloud Certificate Management (Cloud PKI) 478, 523
advantages 522
certificate revocations 535
process, working 523
two-tier PKI hierarchy 524-535
cloud configuration scenario 295-297
app, selecting for deployment 299
assignments 300
deploying 301-303
devices, monitoring 303
essentials, deploying 303
need 297
resources 298
Windows Autopilot settings specific, configuring 297
Cloud Management Gateway (CMG) 37
client apps 40, 41
compliance policies 37
device configuration 39
endpoint protection 38, 39
Office Click-to-Run apps 40
resource access policies 38
Windows Update for Business (WUfB) 37
cloud native
paths to 25, 26
cloud-only groups 68
Cloud PC 96, 107
Conditional Access management 150-152
connecting, with Windows App 152-156
GPU-Enhanced Cloud PCs 110
licenses 108-110
local administrator permissions 149
notifications for failed provision, configuring 706-709
on-premises network, connecting to 111, 112

overview 683
provisioning 133-139
provisioning, creating 140-147
reprovisioning 148
security baselines 149
Windows Autopatch, enabling for 244

Cloud PC encryption type 677

Cloud PC watermarking 678

cloud printers
assigning and deploying, with Microsoft Intune 752-755

Cloud Solution Provider (CSP) 251

co-management 201-207
supported, workloads 37

co-management settings 208
configuring, into Autopilot 208, 209

Comma-Separated Values (CSV) 251

Common Name (CN) 377

community events
MEM Summit - Paris 768
MMS - Minnesota and Fort Lauderdale 768
Windows 365 Community 769
Windows in the Cloud - video webcast 769
Workplace Ninja Summit - Europe 769

company domain CNAME registration
testing, for Windows enrollment 191-193

compliance deadlines
enforcing, for updates 211

compliance policies 37, 463, 661
device compliance trends 472
device diagnostics settings 472-474
devices 464
organizational compliance report 469-471
settings 463
Windows compliance policy 464

Conditional Access 605
common decisions 606, 607
common signals 606
configuring, for Remote Help 557-562
grant settings 612-615
user and groups 607, 608

Config Refresh 455, 456

Configuration Manager 105
co-management 105
disaster recovery 107
fixed-price licenses 108-110

Configuration Manager data collection 699

Configuration Service Provider (CSP) 272, 389, 422, 638

conflicting policies
handling 211

Content Delivery Network (CDN) 40

ControlUp Enrich 712

Copilot assistant
for Intune device queries 588

Copilot, in Windows 576

CSP policy 389-393

customer-managed keys (CMKs) 726

custom images, with Windows 365
reference link 114

D

Data Recovery Agent (DRA) 288

device configuration 39

device configuration with templates
configuring 451-453
custom policy, leveraging 453-455

Device Firmware Configuration Interface (DFCI) 451

Device Health Attestation (DHA) 464

Device query 567-569

devices
enrolling 190
resetting 314, 315

Direct Memory Access (DMA) 281

disk encryption 415

driver updates 210

E

email notifications 706

endpoint analytics 16, 17, 682
insights and recommendations 698

endpoint analytics, advanced monitoring 684, 685
cloud PC, resizing 690-692
performance score 687-690
startup performance 686

Endpoint Detection and Response (EDR) 10, 38, 415, 659

Endpoint Privilege Management (EPM) 478, 481
configuring 481, 482
devices, onboarding into 482
elevation setting policy, configuring 482-486
end user workflow 505-508
features 481
policy, configuring for standard user 503-505
reusable settings 486-490
reusable settings, configuring 490

endpoint protection (EPP) 10, 38, 39

endpoint scenarios 56

endpoint security disk encryption 38

endpoint security profile
Antivirus reporting, in Endpoint security 418
configuring 415
Microsoft Defender policy 416-418

enrollment notifications 194
creating, for Windows 195-199

Enrollment Status Page (ESP) 193, 194, 272
implementation, Windows CSP 272-275

Enterprise App Management 478, 508
applications, installing via 509-517
enhanced application updates 517-522

Enterprise Mobility Management (EMM) 26

Entra ID device registration
users, preventing from carrying out 616, 617

EPM Agent 502

EPM elevation report 499
elevation report by Applications 500
elevation report by Publisher 501
elevation report by User 501
managed elevation report 500

EPM elevation rules policy
creating 491-496
Get-ClientSettings 499
Get-DeclaredConfiguration 496
Get-DeclaredConfigurationAnalysis 497
Get-ElevationRules 498
Get-Policies 496

EPM events
monitoring 499

European Economic Area (EEA) 18

Exchange Online 22

existing Windows devices
deploying, into Microsoft Intune 189, 190

Extended Attributes (EAs) 650

Extended Security Updates (ESUs) 45

F

factory reset 314

Fast Identity Online (FIDO) 150

feature updates 210

feature updates for Windows 10 and later 224, 225
configuring 226-229
prerequisites 225
safeguard holds, opting out 229, 230

File hash 495

Firewall 38, 415

Firmware Over-the-Air (FOTA) 478

first-line worker (FLW) 293

G

General Data Protection Regulation (GDPR) 212, 726

Generic Volume License Keys (GVLKs) 43

golden image 140

GPU-Enhanced Cloud PCs 110

Graph Explorer
signing into 266-271

Group Policy Object (GPO) 77, 412

H

Hardware Security Testability Specification (HSTI) 281

HP Connect 31-33
BIOS update policies types, supported by 35
reference link 35

Hybrid Autopilot
avoiding, reasons 201

Hybrid Entra ID configuration
enabling, via Universal Print connector 744, 745

Hybrid Entra ID join 594, 596-601

Hybrid Microsoft Entra join 111

I

Independent Software Vendor (ISV) 88, 374

Intelligent Security Graph (ISG) 644

Internet Printing Protocol (IPP) 716

Intune admin center 41

Intune Administrator licensing 66, 67
Azure Virtual Desktop, using with Microsoft Intune 71-74
Company Portal website, customizing 80
device limit restrictions, for Windows 78-80
enrollment restrictions, creating for Windows 74-76
Entra group-based licensing 68
Intune app, customizing 80
Intune Company Portal apps, customizing 80-83
MDM, setting 68
personal Windows devices, blocking 76, 77
Windows automatic enrollment, enabling 69-71

Intune and Windows 365 experts 763-767

Intune Copilot 14

Intune filters
Compliance Administrator 59
Compliance Data Administrator 59
Intune Administrator 60
Message Center Reader 60
Security Administrator 60
Security Operator 60
Security Reader 60
using, for assigning 57-59

Intune Suite 477
benefits 478
Endpoint Privilege Management 182
Enterprise App Management 183
features 478
prerequisites 479
Remote Help 184
working with 479-481

IntuneWin
using, via Windows app (Win32) 328-341

K

Keylogger protection 676

Key Storage Provider (KSP) 544

Known Folder Move (KFM) 19, 446

Kusto Query Language (KQL) 569

L

legacy policies
handling 211
licensing requirements 61
line-of-business (LOB) applications 6, 322, 323, 716
AppX, deploying via 322-327
MSI, deploying via 322
MSIX, deploying via 322
local user group membership 39
local Windows Firewall
configuring, for Remote Help 554-557

M

MAM user scope 70
managed device
accessing, remotely 552-554
master image 320
Media Access Control (MAC) 256
Microsoft 365 admin center portal 28
Microsoft 365 Apps
customizing 360
deploying 347, 348
Microsoft 365 Apps Admin Center 352
Microsoft 365 Apps customization 360, 361
Office Customization Tool 350-352
update channels 348, 349
updating 238
Microsoft 365 Apps Admin Center 352-355
device selection criteria 355
device selection criteria, Channels section 356
reference link 350
Update deadline menu 357-360
update exclusion dates, selecting 356, 357
Microsoft 365 Apps for Enterprise 18
Microsoft 365 apps, updating options
administrative templates, to configure policies 238
servicing profile 238
Microsoft 365 cloud services 3
Microsoft Azure Attestation (MAA) 464
Microsoft Defender for Endpoint 21, 22, 659, 663-666
Exchange Online 22
integrating, with Microsoft Intune 659
SharePoint Online 22
Microsoft Defender Security Center
options 676
security recommendations 676
Microsoft Deployment Toolkit (MDT) 190, 260
Microsoft Edge 20, 21
deploying 365-367
features 21
Microsoft Entra admin center
URL 558
Microsoft Entra ID (Entra ID) 5, 27, 36, 41, 191, 595, 716
features 595
group membership types 603-605
group types 603
guest users 602
passkeys 626
passkeys, benefits 627
passkeys, enabling 627-629
passkeys, managing 629
passkeys, usage 626
passwordless authentication, enabling 622-624
passwordless scenario, considerations 624-626
passwordless sign-in authentication 619-621
password protection 618, 619
users 601, 602
web sign-in 630-632

Microsoft Entra ID Join 593, 595, 596
features 596
Microsoft Entra join 111
Microsoft Identity 593-595
Microsoft Identity Management (MIM) 598
Microsoft Installer (MSI) 273, 322
Microsoft Intune 4, 5, 26-28, 98, 594
access, granting 6
achieving, tasks 6
application delivery 319
architecture 26
cloud printers, assigning and deploying 752-755
connecting to 667-676
existing Windows devices, deploying into 189, 190
HP Connect 31-35
integrating with 659
modern management 98
monitoring and analytics capabilities 181, 182
on-premises-to-cloud 42
Partner portal 29
Remote Help, configuring 547-549
required web browser versions 63
roles and privileges, identifying 56
service portfolio 5
supported OSes 62
Surface Management Portal 29, 30
Windows 365 35, 36
Windows 365, working with 103, 104
Microsoft Intune admin center portal 28
Microsoft Intune Security blade
policy, configuring 412-415
Microsoft Intune Suite 7
features 7
Microsoft-managed keys (MMKs) 726
Microsoft Management Console (MMC) 541
Microsoft product updates 210
Microsoft recommended driver block rules
reference link 508
Microsoft Teams 19, 20
deploying 361-363
features 19
Microsoft updates 48
Mobile Application Management (MAM) 21
Mobile Device Management (MDM) 26, 69, 191, 265, 388, 540, 596
Monthly Enterprise Channel (MEC) 44
MSIX 372
advantages, of packing application as 372
AppxBlockMap.xml package 374
AppxManifest.xml package 374
AppxSignature.p7x package 374
packages, creating 374-382
MSIX package application
pushing, to endpoints 382-385
multi admin approval 459-463
Multi-factor Authentication (MFA) 36, 595
multiple Cloud PCs 174

N

network URL firewall requirements 83
managed devices access, providing 84-86
Microsoft Store endpoint URLs 88
network requirements, for PowerShell scripts and Win32 apps 86, 87
Windows 365 and Azure Virtual Desktop 89
Windows 365 endpoint URLs 88
Windows Push Notification Services 88
non-deferrable Windows updates 216

O

Office Click-to-Run apps 40
OneDrive
deploying 364, 365
Microsoft Edge, deploying 365-367
specific file extensions, block syncing 450

OneDrive cloud backup 19

OneDrive folder backup 19

OneDrive for Business 18, 19

on-premises network connection 111, 112
custom images 114
GPOs, migrating to Settings Catalog policy 120
optimized Teams 119
provisioning policy 112, 113
roles and delegation 115-117
screen capture protection 119
Watchdog service 117
watermarking 120
Windows 365 gallery images 113, 114
Windows Updates, via Autopatch 114

Open Mobile Alliance Device Management (OMA DM) 389

Operating System (OS) 387, 678, 717

original equipment manufacturers (OEM) 733

OS restart history 694

out-of-box experience (OOBE) 190, 263
Windows updates 264, 265

P

passkeys 626
benefits 627
enabling 627-629
managing 629
saved list, filtering by name 630
usage 626

pass-the-hash (PTH) 639

passwordless authentication 619-621
enabling 622-624

Personal Data Encryption (PDE) 38, 636-638
Application Control for Business 644-659
Windows Local Administrator Password Solution (LAPS) 638-644

PKI requirements
reference link 544

PKI, securing
reference link 546

Platform Configuration Register (PCR) 464

policy design 398-401

policy management 387, 388, 412
attack surface reduction (ASR) 419-421
policy, configuring from Settings catalog 422-438
unhealthy endpoints 418, 419

PowerShell scripts
pushing 456-458

Preboot Execution Environment (PXE) 190

print support application (PSA) 721

Productivity Score 15, 16
Endpoint analytics 16, 17

Proof of Concept (POC) 389

provisioning policy 112

Q

quality updates 210

R

recommendation for key management
reference link 546

Recovery Point Objective (RPO) 107

Recovery Time Objective (RTO) 107

redirection, per endpoint platform 160
device redirection 161
display configuration 161
identity redirections 163
ports redirections 162
Windows effects configuration 160

remediation script 701-704

Remote Help 478
Conditional Access, configuring for 557-562
configuring, in Intune 546-549
local Windows Firewall, configuring for 554-557
using, as end user 563
using, as ServiceDesk user 563

viewing, from end user's perspective 550, 551
Remote Help for Windows 546
resource access policies 38
resource performance 694
role-based access control (RBAC) 601
roles and privileges , Windows 365 cloud PC
Azure Subscription Owner 61
Domain Administrator 61
Round Trip Time (RTT) 697

S

safeguard holds 223, 224
score trends 695
screen capture protection 678
security baselines 660, 661
Security Copilot 14, 582
Intune policy generation via 582-587
Intune, troubleshooting via 588-591
Security Identifiers (SIDs) 504
self-deploying mode 306
custom Windows 10 profile, creating to disable FirstLogonAnimation 307
custom Windows profile, creating to disable user ESP 307
Windows template SharedPC profile, creating 308-310
Self-service Password Reset (SSPR) 617, 618
service connection point (SCP) 600
service health 709, 710
Service-level Agreement (SLA) 107
setting assistant feature 584
SharedPC self-deployment scenario 303
Self-Deploying (preview) 306
SharedPC technical reference 310-312
specific ESP, creating 303-305
Windows Autopilot profile, creating 305, 306
Windows Autopilot Reset 312-314
SharePoint Online 22
Simple Certificate Enrollment Protocol (SCEP) 273
Single Sign-On (SSO) 595, 596, 718
Snipping Tool 65
Software as a Service (SaaS) application 608
Specialty Device Management 478-481
standard user
policy, configuring for 503-505
startup performance process 692
Stock-Keeping Unit (SKU) 690
Subject Matter Experts (SMEs) 523
supersedence mode 342-347
Surface Management Portal 29, 30
system alerts 706
System Center Configuration Manager (SCCM) 201, 260, 388
System Management Basic Input/Output System (SMBIOS) 251
System on a Chip (SoC) 63
system tray (systray) 65

T

tenant attach 27, 36, 41, 189, 202-207, 699
Threat & Vulnerability Management (TVM) 466
Total Cost of Ownership (TCO) 98
Trusted Platform Module (TPM) 283, 464, 465, 543, 632
Trusted Platform Module (TPM) 2.0 11
Tunnel for Mobile Application Management 478
two-tier PKI hierarchy 524-535

U

Unified Extensible Firmware Interface (UEFI) 11, 281, 451
Universal Print 21, 89, 715

architecture overview 717, 718
benefits 716
configuring 734-743
connector 722, 723
custom roles 732, 733
Delivery Optimization 90
deployment steps 731, 732
end user requirements 728
existing printer, configuring 733, 734
for Mac 718
for Windows 718
network requirements 730, 731
printed data, considerations 724, 725
printer and printer share, testing 749-752
printer defaults 724
printer share, creating for printer 745-749
printer shares 723
ready printers 719-722
requirements 728, 729
requirements, managing 729
roles and privileges, identifying for 61
secure release options 727
security 724, 725
web applications and print APIs 719

Universal Print connector 717
Hybrid Entra ID configuration, enabling via 744, 745

Universal Print, print jobs
compliance and certifications 726
Data Residency policies 725
data security 726
printer share access check 727
secure release 727, 728

Universal Print ready printers 717

Universal Print service 717

Universal Windows Platform (UWP) 322

Update deadline menu 357

update rings for Windows 10 and later 225
creating 213

updates, types managed by Windows Update for Business 210
driver updates 210
feature updates 210
Microsoft product updates 210
quality updates 210

upgrades 48, 210

users' account type
obtaining, to Standard 502, 503

V

Virtual Desktop Infrastructure (VDI) 7, 35

Virtual Hard Disks (VHD) 372

virtual local area network (VLAN) 723

virtual machine (VM) 723

Virtual Network(s) (VNets) 124

Virtual Private Network (VPN) 38

W

Watchdog service 118

web applications and print APIs 719

web sign-in 630-632

Windows
Universal Print 718

Windows 11 10-12
availability 66
download link 190
hardware requirements 63-65
identity access 11
Information Protection 11
release cycle, updating 45, 46
threat protection 10

Windows 11 Enterprise 10, 11
exploring 42
features and services 42, 43

Windows 365 7, 8, 96
battery status redirection 175

complexity, removing while increasing security 97
deploying, requirements 124-132
exploring 184
for non-managed endpoints 52
high-level architecture components 104
low costs, as fixed-price model 97, 98
modern management, with Microsoft Intune 98
OneDrive Known Folder Move feature 97
security baselines 663
service responsibilities 9
services 104
traditional VDI deployments complexity, removing 97
URLs 125
versus Azure Virtual Desktop (AVD) 8
Windows 10 ESUs 99, 100
Windows 365 Enterprise versus Business 100-102
Windows 365 Frontline 102
Windows 365 Government 103
working, with Microsoft Intune 103, 104

Windows 365 and Intune
pairing, reasons 572, 573

Windows 365 Boot
dedicated mode 174
shared mode 163-173

Windows 365 cloud PC
roles and privileges, identifying 61

Windows365 FQDN tag 127

Windows 365 Frontline 704

Windows 365, security baselines
Microsoft Defender for Endpoint 663-666

Windows 365-specific metrics 696-698

Windows 365 Switch 176-178
Cloud PCs, resizing 178

Windows App
Cloud PC, connecting with 152-154
deploying, via Intune 156-158
download link 153, 155
User Actions 159

Windows App Packages (AppX) 322

Windows Autopatch 44, 114, 238
enabling 239-242
enabling, for Cloud PCs 114, 244
requirements 239
Windows Update rings, optimizing 242

Windows Autopilot 40, 190, 200, 201
device information, storage location 257-259
for existing devices 259-264
hardware ID, upgrading to 250-256
overview 248-250

Windows Autopilot profiles
auto-assigning, in Intune 265

Windows compliance policy 464-469

Windows Copilot 12, 14, 576, 577
features 12, 13
using 577-579

Windows Defender Application Control (WDAC) 314, 416

Windows Defender for Endpoint
Cloud PC encryption type 677
keylogger protection 676
screen capture protection and watermarking 678

Windows enrollment 190
automatic enrollment 191
co-management 201-207
company domain CNAME registration, testing 191-193
enrollment notifications 194-199
Enrollment Status Page 193, 194
existing infrastructure 201
tenant attach 201-207

Windows Feedback Hub 237

Windows Fresh Start 315

Windows Hello for Business 11, 290-295

Windows Insider Program for Business 235-237
reference link 236
Windows Local Administrator Password Solution (LAPS) 39, 638-644
Windows patch
expediting 231-235
Windows Push Notification Service (WNS) 88, 231, 391-398
Windows Recovery Environment (RE) 316
Windows Server Active Directory (AD) 39
Windows Server Update Services (WSUS) 47
Windows Stockkeeping Unit (SKU) 49
Windows subscription activation 43, 44
Windows Update for Business (WUfB) 189, 210
companies, benefitting ways 47
configuration setting 47-49
compliance deadlines, enforcing for updates 211
configuring 212-223
conflicting policies, handling 211
deployment service 49
guidelines 223
legacy policies, handling 211
leveraging 47
managing, updates types 210
phases 211
safeguard holds 223, 224
setting up 212-223
using, benefits 210
Windows Update rings 37, 46, 47
optimizing 242
Windows updates
during, OOBE 264, 265
WinGet 368-371

Z

Zero-Day Patch (ZDP) 264
zero trust 50
devices, verifying 50-52
identity, verifying 50